



Priva-cy o no?

Dai programmi di sorveglianza globale ai
tools privacy aware.

ING. ANTONIO PIROZZI

DIRECTOR OF MALWARE LAB @ CSE CYBSEC ENTERPRISE SPA

\$whoami

- M.Sc in Computer Science Engineering
- Director of Malware Research Lab At CybSec Enterprise spa
- ISWATlab co-founder and researcher (www.iswatlab.eu)
- Lecturer for the II level Master in Intelligence and Cyber security at LinkCampus University
- Research and teaching assistant at University of Sannio
- Ec-Council SME and exam item writer
- Cyber Security Consultant for NTTData
- More than 12 International Certification

Andrew Grove - Intel

'Only the Paranoid will Survive''

Thomas Ray

*"Every successful system accumulates
parasites"*

nothing will be as it seems...



Intelligence Gathering

- Open-Source Intelligence (OSINT) refers to a broad array of information and sources that are generally available, including information obtained from the media (newspapers, radio, television, etc.), professional and academic records (papers, conferences, professional associations, etc.), and public data (government reports, demographics, hearings, speeches, etc.).

Cit. Fbi.gov

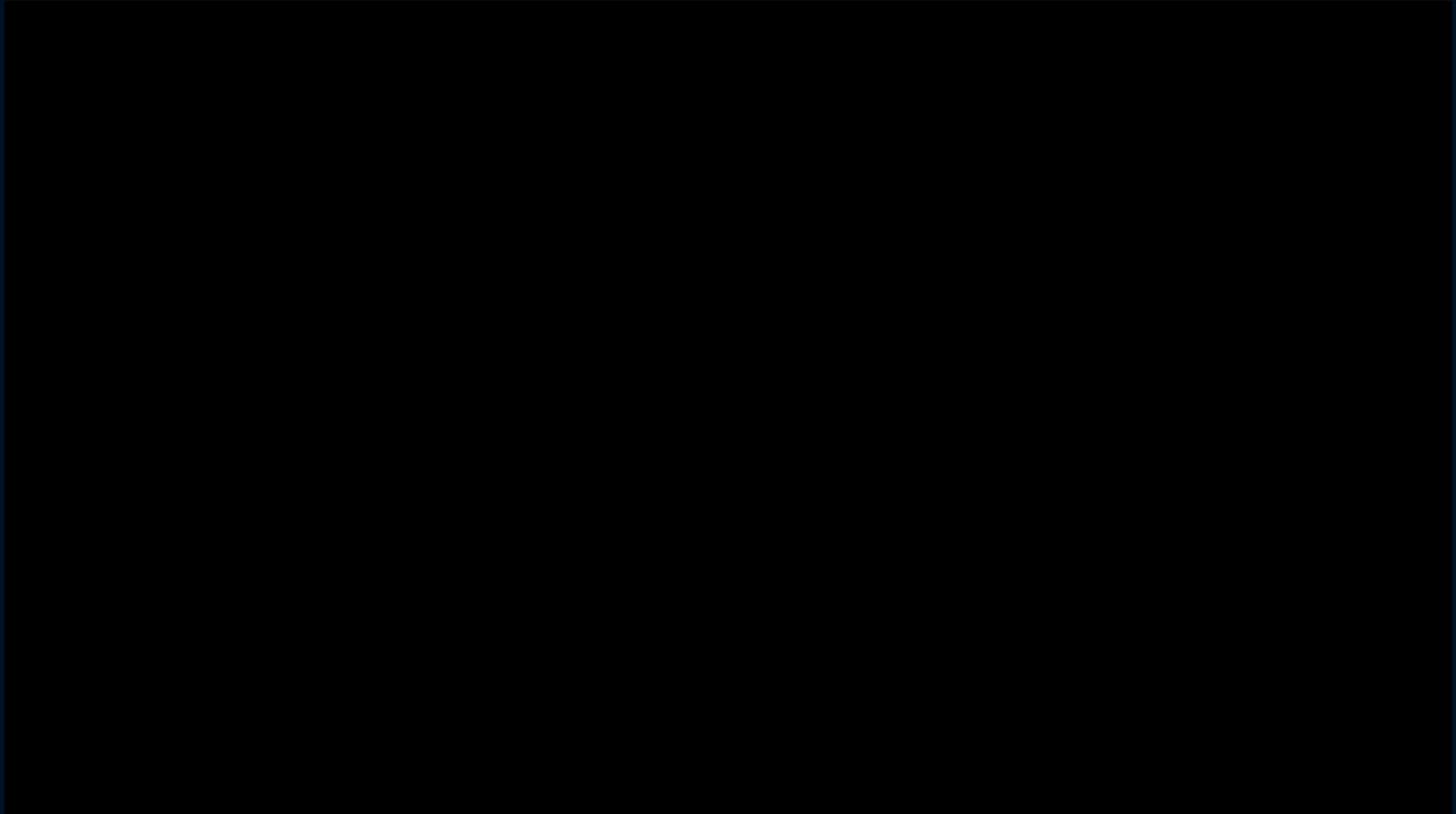
- GEOINT
- SIGINT
- TECHINT
- FININT
- HUMINT

Who collects and use Intelligence

- Law Enforcement
- Military
- Criminals
- Spies
- Government
- Journalists
- Business
- Hackers

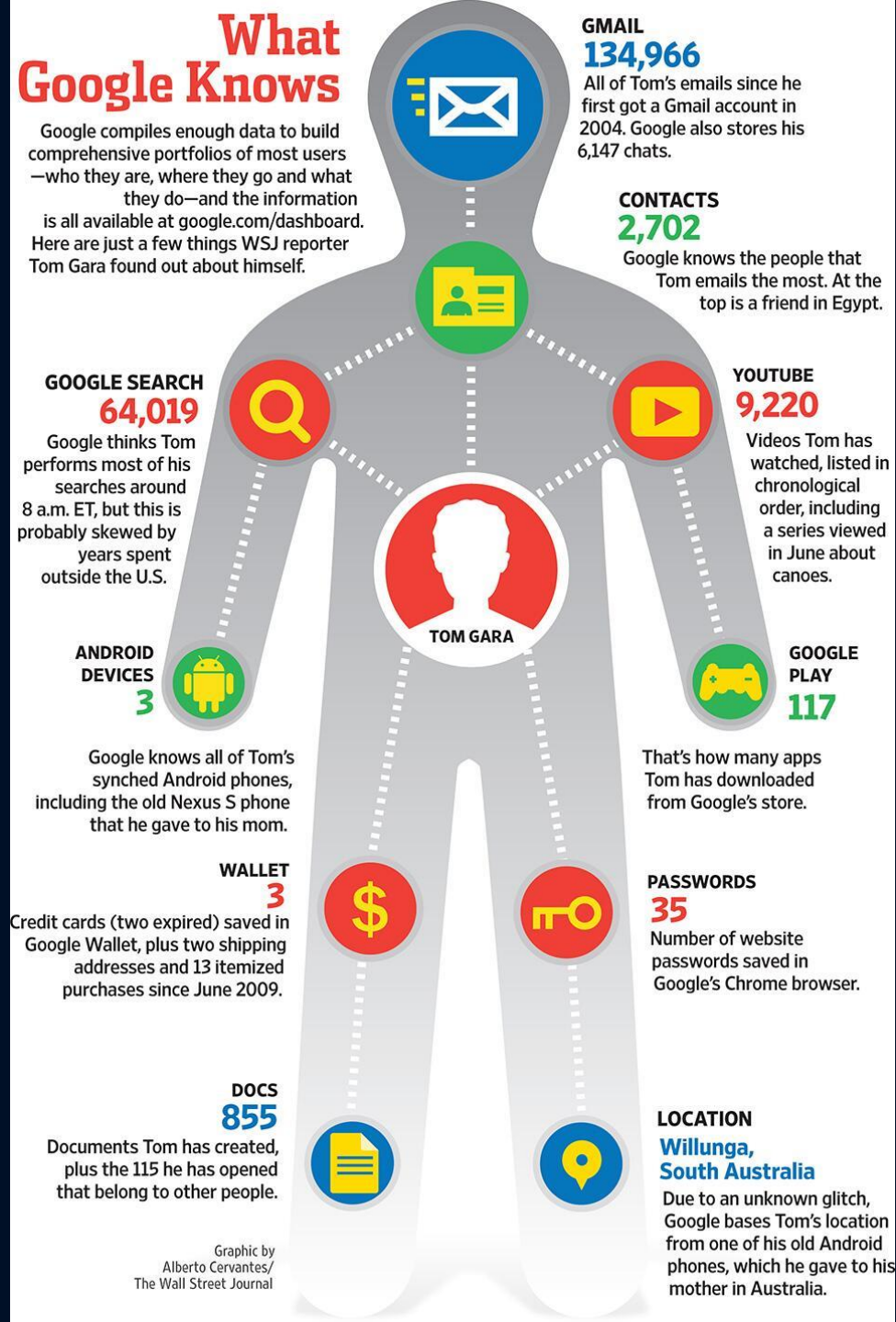


Before we start...



What google knows about you...

- Each entry is time-stamped
- that list is all searchable
- With all that imagined, can you think of a way a hacker, with access to this, could use it against you?
- go over to *google.com/dashboard*, and see it all become reality.



Wikileaks Vault 7

13 July 2017 - CIA HighRise Android malware

19 July 2017 - UCL/RAYTHEON

27 July 2017 - Imperial project

- Achilles - A tool to trojanize a legitimate OS X disk image(.dmg) installer.
- SeaPea - A Stealthy Rootkit for Mac OS X Systems
- Aeris - An Automated Implant for Linux Systems

03 August 2017 - Dumbo tool

10 August 2017 - CIA CouchPotato

24 August 2017 - ExpressLane

31 August 2017 - AngelFire

...



Facebook...



Facebook...

1) Peter Thiel: \$ 500.00 Aug.
2004 (**Palantir's** largest shareholder)



Facebook...

1) Peter Thiel: \$ 500.00 Aug.
2004 (**Palantir's** largest shareholder)



2) \$12.7 million came from James Breyer (Accel Partners)

Facebook...

1) Peter Thiel: \$ 500.00 Aug.
2004 (**Palantir's** largest shareholder)



2) \$12.7 million came from James Breyer (Accel Partners)

3) Greylock Partners → Howard Cox \$25.5 million

Facebook...

1) Peter Thiel: \$ 500.00 Aug.
2004 (**Palantir's** largest shareholder)



2) \$12.7 million came from James Breyer (Accel Partners)

3) Greylock Partners → Howard Cox \$25.5 million



Facebook...



Keyhole Inc

1) Peter Thiel: \$ 500.00 Aug.
2004 (**Palantir's** largest shareholder)



2) \$12.7 million came from James Breyer (Accel Partners)

3) Greylock Partners → Howard Cox \$25.5 million



Facebook...

In 2009, Google Ventures and In-Q-Tel invested
"under \$10 million each



Keyhole Inc



1) Peter Thiel: \$ 500.00 Aug.
2004 (**Palantir's** largest shareholder)



2) \$12.7 million came from James Breyer (Accel Partners)

3) Greylock Partners → Howard Cox \$25.5 million

Facebook...

In 2009, Google Ventures and In-Q-Tel invested "under \$10 million each



Keyhole Inc

1) Peter Thiel: \$ 500.00 Aug. 2004 (**Palantir's** largest shareholder)



2) \$12.7 million came from James Breyer (Accel Partners)

3) Greylock Partners → Howard Cox \$25.5 million



Facebook...

In 2009, Google Ventures and In-Q-Tel invested
"under \$10 million each



Keyhole Inc

1) Peter Thiel: \$ 500.
2004 (Palantir's largest shareh

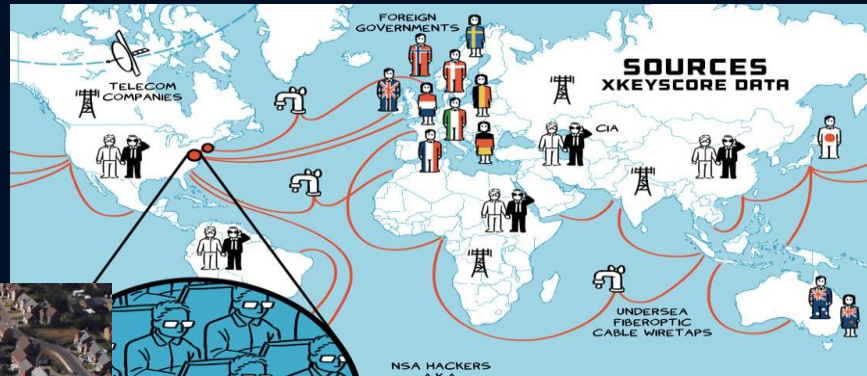


2) \$12.7 million came from James Breyer (Accel Partners)

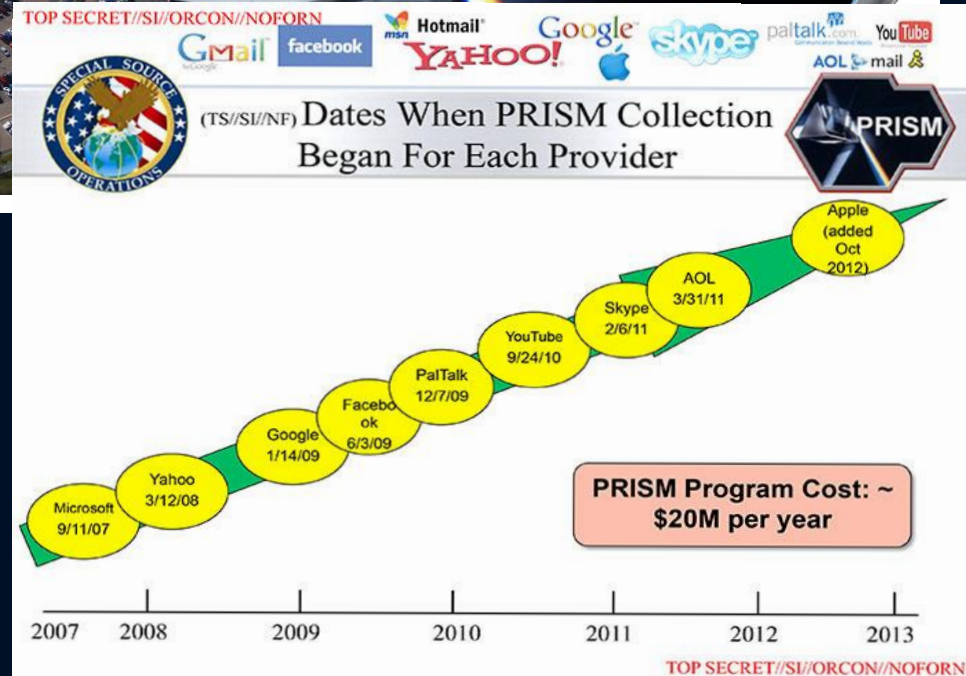
3) Greylock Partners → Howard Cox \$25.5 million



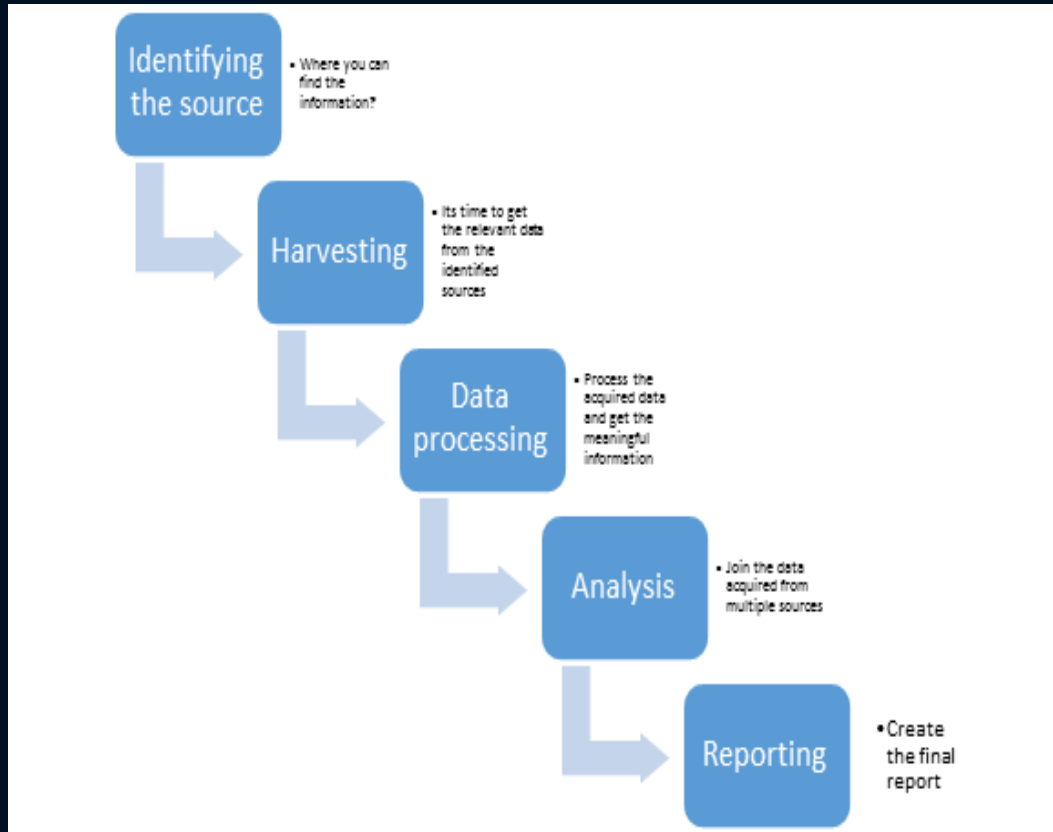
Mass surveillance...



gemalto
security to b



The OSINT Process...

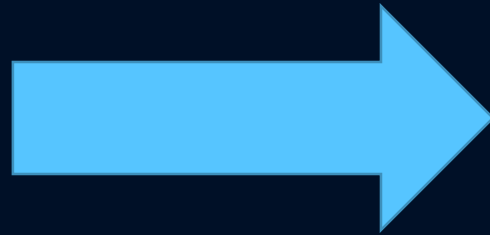


- Hostname
- Services
- Networks
- SW/HW versions and OS information
- Geo-location
- Network diagram
- Database
- Documents, papers, presentations, spreadsheets
- and configuration files
- Metadata
- Email and employee search (name and other personal information)
- Technology infrastructure
- IP

Doxing

Is the Internet-based practice of researching and broadcasting private or identifiable information (especially **personally identifiable information**) about an individual or organization. wikipedia

- Google
- Bing
- Peek you
- Pipl
- Intelius
- Facebook GRAPH
- Shodan



- Name
- Ages
- Email
- Addresses
- Phone numbers
- Photos
- Etc.
- Location
- IP CAMERA & IoT!!!

Google advanced operators

- **Web Search:** allinanchor:, allintext:, allintitle:, allinurl:, cache:, define:, filetype:, id:, inanchor:, info:, intext:, intitle:, inurl:, link:, related:, site:
- **Image Search:** allintitle:, allinurl:, filetype:, inurl:, intitle:, site:
- **Groups:** allintext:, allintitle:, author:, group:, insubject:, intext:, intitle:
- **Directory:** allintext:, allintitle:, allinurl:, ext:, filetype:, intext:, intitle:, inurl:
- **News:** allintext:, allintitle:, allinurl:, intext:, intitle:, inurl:, location:, source:
- **Product Search:** allintext:, allintitle:

personally identifiable information

▶ Website investigation:

- ▶ <https://Pipl.com>
- ▶ <http://www.amazon.com/gp/registry/search/>
- ▶ <http://www.indeed.com/resumes?q=%22PHm%22>

https://www.linkedin.com/vsearch/f?trk=federated_adv_s&adv=true

- ▶ Cached data: <http://archive.org/web/>, google cache,
- ▶ Knowem,
- ▶ checkusernames.com/
- ▶ <https://namechk.com/>

Code:
<https://nerdydata.com>

▶ US only:

- ▶ <http://www.classmates.com/>,
- ▶ <https://www.intelius.com/>,
- ▶ <http://radaris.com/>
- ▶ <http://www.spokeo.com/>
- ▶ <http://www.peakyou.com/>
- ▶ <http://mugshots.com/>

- ▶ <https://emailhunter.co>
- ▶ <https://toolbox.googleapps.com>

▶ Skype

- ▶ <http://www.skresolver.com/>

▶ Companies/ business :

- ▶ <https://findthecompany.com>
- ▶ <http://copyright.gov/>
- ▶ <http://www.keywordspy.com/>
- ▶ <https://www.crunchbase.com>
- ▶ <https://connect.data.com>

▶ Bitcoin :

- ▶ <https://blockchain.info/address/1Kqzbv4ekpJX3ohYWGEzMqzvf27VjBux35>
- ▶ <https://www.blockseer.com/addresses/1Kqzbv4ekpJX3ohYWGEzMqzvf27VjBux35>

personally identifiable information

- The Harvester
- Fb
- Social Media
- Recon-ng
- Metadata



Geo location



- ◆ Gmaps
- ◆ Gearth

Private earth observation satellites:

GeoEye - 5 satellites: IKONOS, OrbView-2, OrbView-3, GeoEye-1, GeoEye-2

DigitalGlobe - 4 satellites: Early Bird 1, Quickbird, WorldView-1, Worldview-2

Spot Image - 2 satellites: Spot 4, Spot 5

SOCMINT

- FacebookGRAPH
- Fbsleep
- Creepy
- <http://www.socialmention.com>

Reverse Image Search

- ▶ Google Image
- ▶ TinEye
- ▶ Yandex
- ▶ Googles (on G Play Store)
- ▶ Findface (on G Play Store)

AD Analytics

*Id <--> domain
correlation*

- ▶ <http://spyonweb.com/>
- ▶ <http://sameid.net/>
- ▶ <https://ewhois.com>

Google AdSense

ca-pub-9158781978326526

```
data-ad-client="ca-pub-9158781978326526" data-ad-
```

UA-6197637-22

```
etElementsByTagName(0,10],a.async=1,a.src=g,m.parentNode.insertBefore  
,document,'script','//www.google-analytics.com/analytics.js','ga');  
  
e','UA-6197637-22','semrush.com');  
re','displayfeatures');  
  
ming=function(){function h(d,c,b){var e="XDomainRequest"in window?"  
h).setTimeout(200).onreadystatechange=function(){h).setTimeout(function()
```

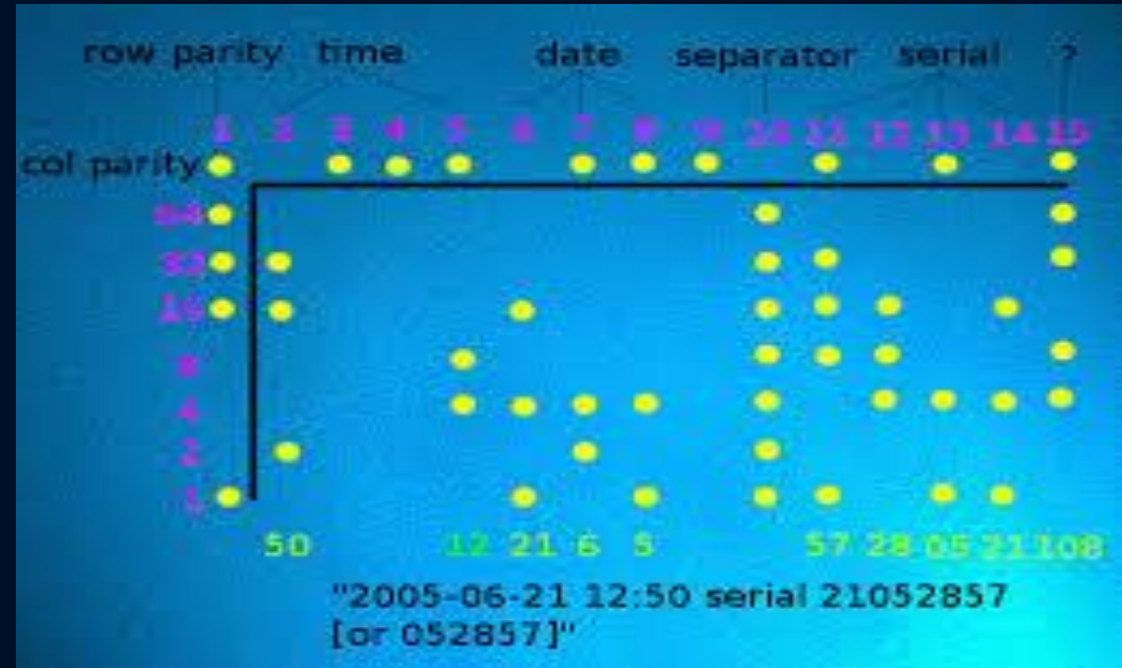
Metadata | 'data about data'

- Foca
- Metagoofil
- Exiftool <exif foto e docs>
http://www.motherjones.com/files/images/war_photo_063010.jpg
- gpg -- with-fingerprint key.asc
- Printers **SRSLY?????**

http://www.repubblica.it/esteri/2015/06/05/news/militante_dell_is_si_fa_un_selfie_e_24_ore_arrivano_3_missili-116096314/

Printers dot CODE

2005 EFF discover it



List of printers:

<https://www.eff.org/it/pages/list-printers-which-do-or-do-not-display-tracking-dots>



PRIVACY

NO PRIVACY ANYWHERE

memegenerator.net





browser fingerprinting techniques




- ▶ HTML5 canvas fingerprinting (obtained in a fraction of a second without user's awareness.)
(**Whitehouse.gov, perezhilton.com**)
- ▶ cookie syncing
- ▶ Evercookies & Respawning (cookies in a web browser that are intentionally difficult to delete / **NSA used it for tracking TOR users**)
- ▶ Local shared objects (LSOs) aka **FLASH cookie**
 - More than 94% of Flash - and Java-enabled browsers can be uniquely identified
 - More he changed his plugins and settings relative to the default,
 - the more unique and easily-identifiable his browser becomes

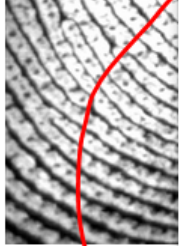
`https://securehomes.esat.kuleuven.be/~gacar/persistent/`


Using HTML5 Canvas To F...
About Tor

    **Future Hosting Technologies LLC (US)**

<https://www.futurehosting.com/blog/using-html5-car>








This website (www.futurehosting.com) attempted to extract HTML5 canvas image data, which may be used to uniquely identify your computer.

Should Tor Browser allow this website to extract HTML5 canvas image data?



common w

containing a unique identifying number, and whenever a browser visits a site that belongs to the advertising network, code on the page looks at the cookie. In this way, advertising networks can track users across the web – and if those users are logged in to a service like Google or Facebook, the tracking can be all the more accurate, because they can associate it with much richer data.

But not everyone is happy with being tracked across the web, and, as web users become more savvy to the privacy implications of tracking, many are choosing to block the third-party cookies used by advertising networks. That's bad news for

CATEGORIES

- BlackFriday (2)
- Business (2)
- Datacenters (18)
- Design (5)
- Global News (8)
- Java (3)
- JBoss (1)
- Misc (23)
- Monthly Content Roundups
- News Releases (8)
- Responsive Design (1)
- Search Engine Optimization

The web NEVER FORGETS:

browser fingerprinting techniques



- ▶ Facebook, Google and Microsoft, will assign a unique identifier to each type of device the user has and link those together to track activity across all of the devices the person uses. These new tracking mechanisms, if they catch on, could be used across each vendor's ecosystem -- and beyond.
- ▶ browser and device "fingerprinting" are *cookieless*

Types of Tracking Solutions on Mobile Platforms

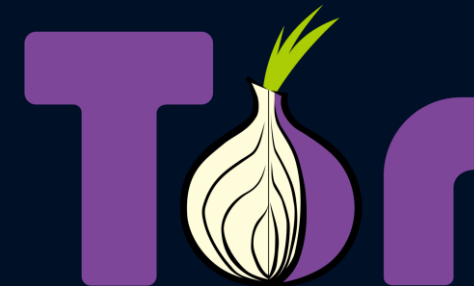
cross-device user identification

- Client- or Device-specific Ids (Users cannot alter or opt out of tracking) :
- from Android ID and iOS UDID to **GAID** for Android, **IDFA** for iOS
-
- SSO
- Cookies on mobile apps

countermeasures



- Do Not Track (DNT)
- Opt-out on DAA
- <http://www.aboutads.info/choices/>
- **Ghostery** Firefox ext.
- **NoScript** of Course!
- Disable third-part cookies
- Adblock plus
- HTTPS Everywhere
- VPN, TOR
- Gtranslate



Any questions?

