

Digital Trail Chasing

Using Open Source Intelligence techniques to find out how much information is public about you and your friends

@spyblog CryptoParty London 25 Jan 2018

Why survey your own data ?

- You cannot use many of the techniques demonstrated at a CryptoParty without first having a good idea of what information about yourself and those close to you might have to protect.
- There will be some public information you cannot do much about, without drastic lifestyle action
- It is often surprising that lots people's personal information is **not** easily available online – yet.

Threat Actors

- What sort of attacker is likely to get your personal data ?
 - High Skill, High Resources, Long Persistence
 - High Skill, Limited Resources, Limited Persistence
 - Low Skill, Limited Resources, Long Persistence
 - Low Skill, Limited Resources, Short Persistence, Luck
- Resources = multiple people & infrastructure
- Persistence = how long will a campaign last e.g. hours, days, weeks, months or years ?

High Skill, High Resource Threats

- High Skill, High Resources / Budget, Long Persistence – months or years
 - Law Enforcement & Intelligence Agencies (UK & Foreign)
 - Only if you are seen as a major threat
 - N.B. Data from Short Persistence, untargeted / collateral “bulk data” scans / exploits likely stored “just in case”
 - Organised Criminal Gangs
 - Only if you are rich or are a vulnerable part of a crime plan e.g. Bank Manager, Systems Administrator

High Persistence Threats

- Low Budget / resources but Long Persistence & maybe Luck
 - Funded Investigative Journalists
 - Hackers
 - Political Activists doing Opposition Research / digging up political dirt
 - Online Trolls / Stalkers / Abusive Ex-Partners
 - Terrorist & Paedophile “groomers” looking for vulnerable victims

Low Budget / Persistence Threats

- Skilled attackers but time constrained due to deadlines or resource limits / finances:
 - Ex LEO / IA working as Private Investigators / Security / Risk / Due Diligence / High Profile Job Recruitment Consultants
 - Freelance Investigative Journalists
 - Tabloid Journalists & Paparazzi
 - Except for bankable Celebrities = Long Persistence

Resources

- **Hunted** on Channel 4 tv - 9pm Thursdays i.e. tonight (hope my recorder is working)
 - <http://www.channel4.com/programmes/hunted>
- The Glass Room – Data Detox
 - <https://tacticaltech.org/news/data-detox-kit/>
- OSINT online tools (not all work on UK people)
 - <https://start.me/p/ZGAzN7/verification-toolset>
 - <https://inteltechniques.com/menu.html>
 - <http://spiderfoot.net/download/>
 - <http://network-tools.com/> - Express option
 - <https://shodan.io> vulnerable Internet of Things et.
 - <https://haveibeenpwned.com/> - check on email / hacked password reuse
- #OSINT hashtag on Twitter
- Google search, Maps, Street View & Bing Maps
- Companies House
- Estate Agents websites (for expensive properties) – photos & floorplans
- “Free” tools often need ReCaptcha completion against scraper scripts

Resources

- Electoral Roll – voter registration – opt out of public version (finance companies & MI5 still get this)
- Have you or target stood for Council or MP etc. election – Home Addresses on Local Council websites of previous Elections
- Estate Agents websites (for expensive properties i.e. almost all London ones) – photos & floorplans

Resources

- Domain Names – current (free) – often need ReCaptcha completion against scraper scripts
 - <https://who.is>
 - <https://ping.eu>
 - <http://network-tools.com>
- For .co.uk or .org.uk or .net.uk or .uk domain names you can Opt Out of the whois if you are **not** using it for trading

Don't be stingy – not everything is free

- Don't be stingy – not everything is “free” – pay a bit of money if your privacy and security are important to you.
- Domain names – historical
 - Domain Tools (£)
 - <https://research.domaintools.com/research/whois-history/>
- .com .org .net etc. domain names cost extra with a whois privacy nominee options

Don't be stingy – not everything is free

- DVLA Registered keeper of a Vehicle
 - Often yields Home Address of Private Vehicles
 - otherwise Company Address / Leasing Company
 - <https://www.gov.uk/request-information-from-dvla>
 - £2.50 per vehicle plus “reasonable cause” e.g. involved in an accident, parking fine etc.

Don't be stingy – not everything is free

- Data Protection Act 1998
 - Subject Data Access Request
 - Currently max **£10 fee** (never any less !)
 - Supposed to reply within 40 days (i.e. usually after 30 day CCTV data retention)
 - Only info about yourself , not other people
 - Can include CCTV footage, emails, database records
 - Public bodies and Private companies including Mobile Phone networks itemised billing with some Location Data

Learn from Tabloid Celebrity Stalking

- Just because The Sun and The Daily Mail have some toxic political views, does not mean that you cannot learn from their Stalking of Celebrities
- James Stunt – billionaire Gold Bullion dealer currently going through alleged £5.5 billion divorce from Petra Ecclestone (daddy's Formula 1 fortune)
 - <http://www.dailymail.co.uk/news/article-5298027/Petra-Ecclestone-flanked-sister-Tamara-arrives-court.html>

Learn from Tabloid Celebrity Stalking

- James Stunt pictured arriving at Court with a Satellite Phone
 - Inmarsat
- Sensational £90 million burglary claim
- Pictures of assistants with bags (washing basket in Luis Vuitton bag)
- Pictures of Lamborghini and Rolls Royce etc. luxury cars
 - <https://www.thesun.co.uk/news/5388659/billionaire-playboy-james-stunt-victim-of-record-breaking-90m-burglary/>
- **No actual Address published** – some Mews house in Belgravia, London – but where exactly ?

Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



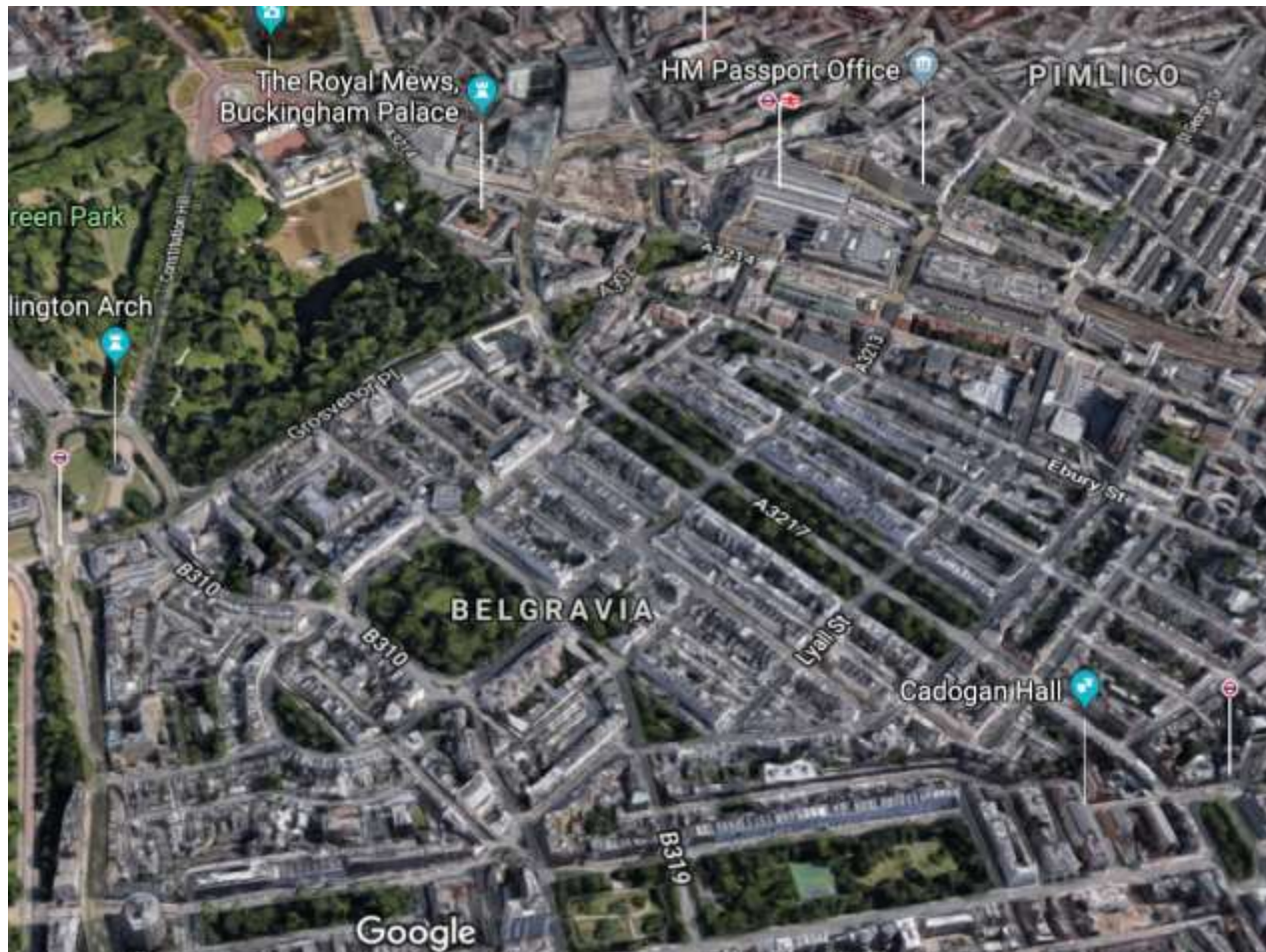
Learn from Tabloid Celebrity Stalking

- Typical Belgravia off white terrace / mews houses
- Note the building at the end of the street i.e. a bend / corner.
- Note the Parking street sign on right and the sign with the arrow on the left
- Note the 6 showing on the column on the right

Learn from Tabloid Celebrity Stalking

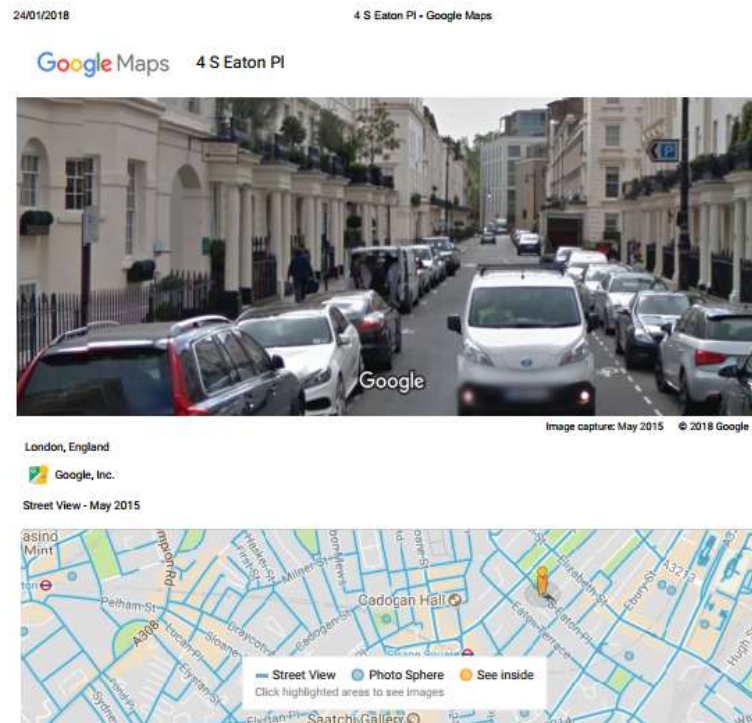
- Try Reverse Image Search
 - <https://www.google.co.uk/searchbyimage/upload>
- and tin eye
 - <https://tineye.com/>
- Nothing useful- just the original photo in The Sun
- Google Maps and Street View allows you to “drive” around Belgravia
- Aerial view lets you find the White painted Mews houses, on not too wide a road.

Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking

- 4 South Eaton Place, Belgravia, London
- <https://goo.gl/maps/1hCiwYtNPfM2>



Learn from Tabloid Celebrity Stalking

- Now try a Companies House search for “James Stunt” <https://beta.companieshouse.gov.uk/>

James Robert Frederick STUNT

Total number of appointments 5 - Born January 1982

Seventh Floor, Leconsfield House, Curzon Street, London, United Kingdom, W1J 5JA

James Robert Frederick STUNT

Total number of appointments 5 - Born January 1982

7th Floor, Leconfield House, Curzon Street, London, United Kingdom, W1J 5AJ

James Robert Frederick STUNT

Total number of appointments 1 - Born January 1982

Leconfield House, Curzon Street, Mayfair, London, England, W1J 5JA

James Robert Frederick STUNT

Total number of appointments 1 - Born January 1982

Henley House, 1a South Eaton Place, Eaton Mews, London, United Kingdom, SW1W 9ES

Learn from Tabloid Celebrity Stalking


- Google search led to RightMove website with a listing and photos and plan of Henley House, 1a South Eaton Place
 - <http://www.rightmove.co.uk/property-for-sale/property-46093549.html>
- Use Firefox i.e. Tor Browser - View Page Info / Media tab - rather than Chrome to grab the 15 individual images of the property

Learn from Tabloid Celebrity Stalking

rightmove [Buy](#) [Rent](#) [Find Agent](#) [House Prices](#) [Commercial](#) [Overseas](#) [Sign In](#)

This property has been removed by the agent. It may be sold or temporarily removed from the market. [View similar properties](#)

4 bedroom character property for sale
South Eaton Place, London, SW1W 9ES Guide Price
£12,000,000




[Market overview](#) [Map](#) [Street View](#) [Picture No. 12](#)

[Description](#) [Floorplan](#) [Map & Street View](#) [Market Info](#)

Key features


- Entrance hall
- reception room
- library/media room
- kitchen/dining room
- master bedroom suite with dressing room and bathroom
- 3 further bedrooms (1 with en suite) and 1 further bathroom
- gym with steam bath and shower
- study, wine cellar, laundry room and guest cloak room
- terrace and 2 parking spaces
- EPC Rating = B

Listing History
Added on Rightmove:
20 September 2018



[Full description](#)
[Location](#)


This property is marketed by:



Savills, Soane Street
139 Soane Street, London, SW1X 8AP
[View properties from this agent](#)

[Save property](#)
[Add notes](#)
[Print](#)
[Send to friend](#)

Share this property



Properties sold nearby

- 20 Sep 2017
13 South Eaton Place, SW1W
£6,425,000
- 10 Dec 2004
9 South Eaton Place, SW1W
£2,635,000

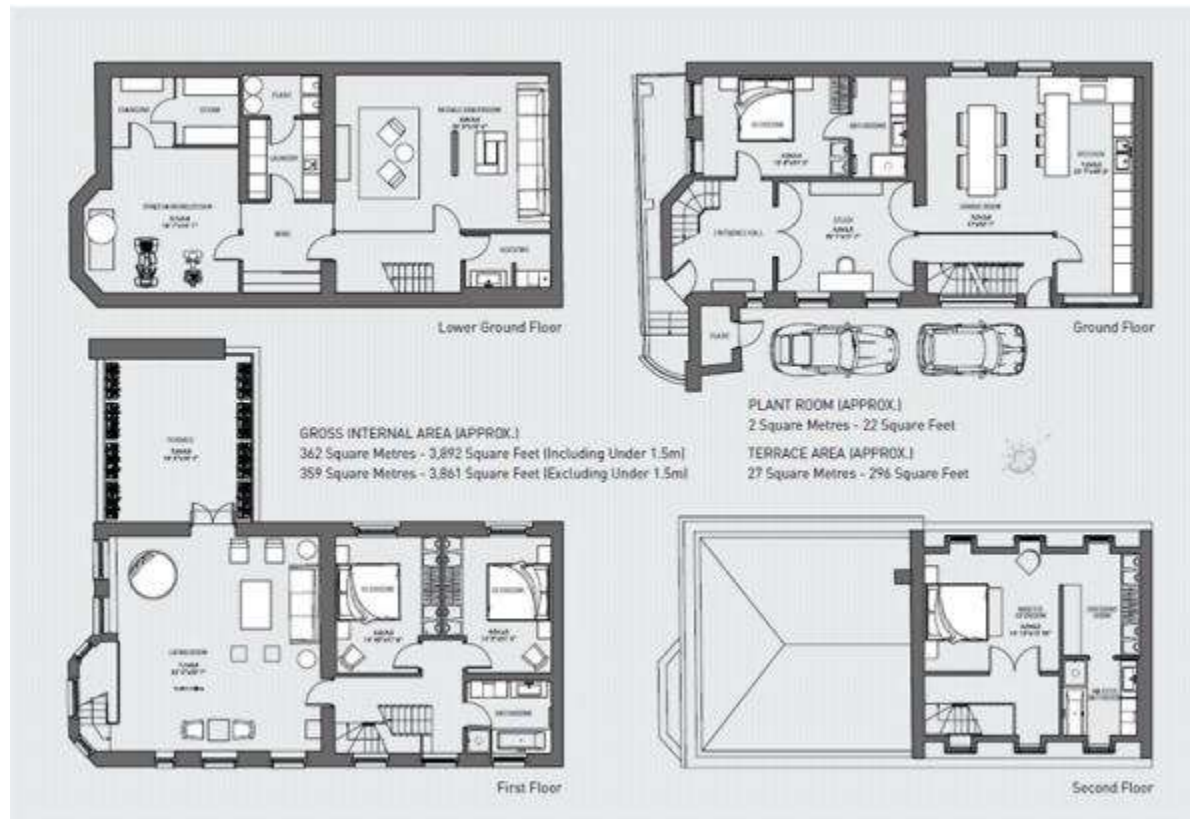
[View more](#)

Helping you stay secure online
Finding a new place to live needn't be stressful. Especially when you're well informed. Visit our security centre to find out more.

Surrounding Areas

- SW1
- Westminster
- London

Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking



Learn from Tabloid Celebrity Stalking

