

Anti-Surveillance Capitalism

CryptoParty London

1st May 2018

<https://cryptoparty.in/london>

@cryptopartyLDN

People of the World Encrypt!


CRYPTOPARTYLDN - TUESDAY 1ST MAY 2018 - WORKERS DAY EDITION - ENCRYPT EVERYTHING

PEOPLE OF THE WORLD ENCRYPT!

FREE WORKSHOPS, TALKS, MUSIC - SURVEILLANCE SELF-DEFENCE - PRIVACY & DIGITAL RIGHTS

1ST MAY
630PM TIL LATE
JUJU'S BAR & STAGE
15 HANBURY ST, E1 6QR

DJ SET BY RJHODE



BRING

charger laptop phone



MORE INFO
<https://cryptoparty.in/london>
@cryptopartyLDN

ANONYMITY | INFOSEC | ENCRYPTED CALLS | SIGNAL | HTTPS | PUBLIC KEY CRYPTO | FREE SOFTWARE | TAILS | QUBES | SUBGRAPH | ENIGMAIL | LIGHTNING TALKS | WORKSHOPS | ENCRYPTION | OPEN SOURCE & FREE SOFTWARE | BITCOIN | TOR | SAFE BROWSING | PASSWORDS & 2FA | PGP

Surveillance Capitalism

- “Surveillance capitalism’ was the term coined in 2015 by Harvard academic Shoshanna Zuboff to describe this large-scale surveillance and modification of human behaviour for profit. It involves predictive analysis of big datasets describing the lives and behaviours of tens or hundreds of millions of people, allowing correlations and patterns to be identified, information about individuals inferred, and future behaviour to be predicted.”
- <https://www.opendemocracy.net/uk/jennifer-cobbe/problem-isn-t-just-cambridge-analytica-or-even-facebook-it-s-surveillance-capitali>
- Google, Facebook, Twitter etc. offer useful “free” services but also make money from it. Directly or indirectly our own and foreign Government agencies and criminals exploit this Big Data against individual privacy conscious people.

Anti-Surveillance Capitalism

- CryptoParty workshops and talks try to help you to protect your privacy and security against some of the threats posed by such massive online surveillance, using tools like encrypted messengers e.g. Signal and email accounts e.g. ProtonMail.
- As a security measure and as a marketing / surveillance tool, many of these now require the use of a landline or mobile phone, at least during the initial installation and setup of the software

“Anonymous” Encrypted Email ?

- Sign up for an encrypted Protonmail email account at <https://protonmail.com>
- Enter the name of your favourite James Bond super-villain planning world domination / revolution e.g. Ernst Stavro Blofeld
- Use a strong passphrase e.g. generated using DiceWare
<https://en.wikipedia.org/wiki/Diceware>

“Anonymous” Encrypted Email ?

5

Are you human?

To fight spam, please verify you are human.

Your email or phone number will not be linked to the account created. It is only used during the signup process. A hash will be saved to prevent abuse of the ProtonMail systems.

- Email**
- SMS**
- Donate**

Email verification

SEND

COMPLETE SETUP

“Anonymous” Encrypted Email ?

- The antispam “security” options given by Protonmail (and Google Gmail etc.) are
 - Give out another traceable email address ?
 - Receive an SMS text message to your financial and location trackable mobile phone ?
 - Pay money electronically leaving an audit trail ?
- These are normally ok, but *not* when you want or need to remain private and / or hard to trace

Anti-Surveillance Capitalism

- Some Common Sense Hints and Tips to help break some of the Digital & Financial & Witness trails which might identify you or your confidential sources and contacts to well resourced state or corporate or criminal investigators

Anti-Surveillance Capitalism

- Avoid drawing attention as you purchase
- Avoid CCTV surveillance (very hard)
- Oyster Travel Card Swaps
- Mobile Phone Swaps
 - Prepaid SIM Cards
 - Prepaid Mobile Phone Top Up Vouchers
 - Unlocked “Burner” mobile phone handsets
- Mobile Phone source protection tips
- Webmail & Social Media accounts

Anti-Surveillance Capitalism

- Avoid drawing attention to yourself as you make a purchase
 - Use Cash (but not large denomination banknotes forcing shop staff to find change or perform anti-forgery checks)
 - No Credit Cards
 - No Contactless Payments
 - No Cheques
 - No Supermarket Loyalty Cards e.g. Nectar
 - No online purchases involving couriers e.g. Amazon

Anti-Surveillance Capitalism

- Avoid drawing attention to yourself as you make a purchase
 - Avoid CCTV surveillance if possible
 - Choose a small retail shop which might not retain CCTV images for more than a month without overwriting them
 - Wear a baseball cap etc. which at least partially hides your face from CCTV cameras usually mounted above you
 - Do not wear distinctive clothing, or easily tracked corporate branding logos
 - Hide any visible tattoos etc.

Anti-Surveillance Capitalism

- Avoid drawing attention to yourself as you make a purchase
 - No Bulk Purchases
 - Shop staff are more likely to remember these
 - Some Supermarkets etc. have unadvertised “fair trading” policies which require supervisory management approval for bulk purchases (i.e. more than one per customer) of “special offer” items
 - Switch off your Mobile Phone well before approaching the retail shop & until you are far away from it

Anti-Surveillance Capitalism

- All of the above warnings and inconvenient precautions can be done away with if you can act as a human cut out and take your purchases to e.g. CryptoParty London to **swap or barter** anonymously / deniably with strangers you met in a bar

Anti-Surveillance Capitalism

- Oyster Card
 - Paying a Bus or Tube fare by cash is now
 - Deliberately more expensive
 - Certain to expose you to more CCTV camera coverage & transport staff memory
 - Vulnerable to leaving forensic clues to your identity via fingerprints, DNA samples, fibre & dust etc.

Anti-Surveillance Capitalism

- Oyster Card

- Oyster Card is a passive RFID smart card, which can be interrogated and time / location / Serial Number tracked silently by rogue Card reader devices up to a range of about 2 to 5 metres
- Genuine Oyster Card readers are tuned down to a range of a few centimetres e.g. to avoid cross talk between adjacent Tube gates

Anti-Surveillance Capitalism

- Foiling the Oyster Card
 - When not in use you can cheaply and effectively block the RFID Oyster Card reader signal which powers up the Oyster Card with aluminium cooking foil in the plastic wallet
 - It is not necessary to wear a “tin foil helmet” !



Anti-Surveillance Capitalism

- Oyster Card
 - Transport for London uses the travel data it collects anonymously from Oyster Card usage to help plan its timetables & services etc. – fair enough
 - TfL used to comply with narrowly targeted requests from the Police & Intelligence Agencies for this data in specific investigations – fair enough

Anti-Surveillance Capitalism

- Oyster Card
 - Congestion Charge ANPR & CCTV data as well as any registration and credit card etc. payment data, is **no longer protected** by the Data Protection Act
 - It is handed over “in bulk, in real time” to the Metropolitan Police for secret “pattern matching” / Data Trawling of millions of innocent journeys.

Anti-Surveillance Capitalism

- Oyster Card
 - This was inflicted on us by Labour Home Secretary Jacqui Smith in 2007 by Ministerial Certificate (with no debate) and has still not been revoked.
 - Ministerial Certificate signed 4th July 2007:
[DPA/s.28/MPS/2007/CC1](#)
 - <http://webarchive.nationalarchives.gov.uk/+http://www.homeoffice.gov.uk/about-us/freedom-of-information/released-information/foi-archive-crime/7393-DPA-real-time-cameras/7393-certificate-1998?view=Binary>

Anti-Surveillance Capitalism

- Oyster Card
 - We have to assume that Oyster Card data is also being handed over to the Police etc. for the same sort of “national security pattern matching” to (foolishly) try detect “suspicious” behaviour patterns amongst the mostly innocent travelling public.

Anti-Surveillance Capitalism

- Oyster Card Swaps
 - One way to confuse the Data Trawling is to regularly **Swap** your Oyster Travel Card with someone else, who has a different pattern of travel.
 - This does **not** affect TfL's transport **planning**, but should help to confuse the Metropolitan Police & UK or Foreign intelligence agencies who have access to Oyster Card travel pattern & payment data
 - N.B. if you are the target of a specific investigation, they will soon overcome any confusion, but at extra cost , so it could be enough to confuse their Data Trawling and prevent you from being generally targeted in the first place.

Anti-Surveillance Capitalism

- Oyster Card Swaps:
 - Buy Pre-paid Oyster Cards at a Tube Station or other retail outlet, ideally without much CCTV or attentive staff
 - £5 deposit + £5 minimum top up = £10
 - Do not buy or register the Oyster Card online
 - Swap your Oyster Card for another unused one with someone at this event

Anti-Surveillance Capitalism

- Oyster Card Swaps:
 - Swap already used Oyster Cards
 - settle up any minor unused credit differences
 - Wipe fingerprints & DNA samples etc.
 - Line the plastic wallet with aluminium foil (against faulty official readers & sneaky commercial or other snoopers)
 - Repeat regularly
 - Do not forget to make some use of the Oyster Card within 6 months or it will get cancelled

Anti-Surveillance Capitalism

– Mobile Phone Swaps

- Prepaid SIM Cards
- Prepaid Mobile Phone Top Up Vouchers
- Prepaid Mobile Phone Top Up Magnetic Swipe Cards
- Cheap, disposable “Burner” Mobile Phone handsets

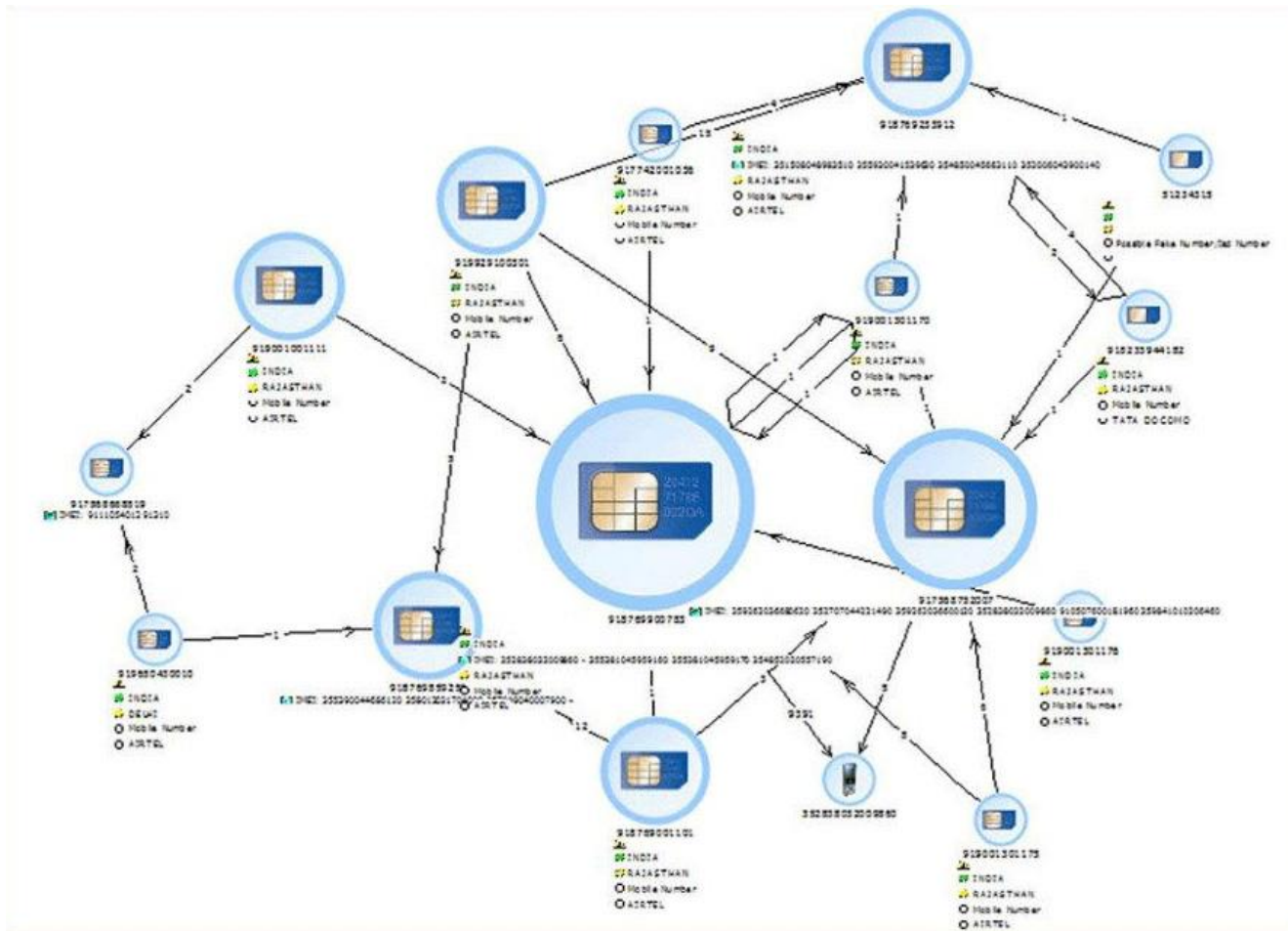
Anti-Surveillance Capitalism

- Prepaid SIM Cards
 - Unlike some other European Union countries e.g. Germany or Spain, it is still legal to buy an unregistered Mobile Phone SIM card in the United Kingdom
 - Most Supermarket Phone Shops offer Prepaid SIM Cards for 99p each and there are also various “free SIM Card” offers
- Avoid drawing attention to yourself as you make a purchase

Anti-Surveillance Capitalism

- What you are trying to achieve is to break the link between Communications Data / MetaData / Traffic Data and your physical identity which may be traceable via financial purchase records or CCTV footage etc.

Anti-Surveillance Capitalism



Anti-Surveillance Capitalism

- Prepaid Mobile Phone Credit Top Up Vouchers
 - Do **not** use
 - » Supermarket Loyalty Card
 - » Credit Card
 - » Contactless Payments
 - » Automated Teller Machine to purchase Mobile Phone Credit the transaction will be linked to your bank account details
 - » Internet Banking website for the same reason
 - Minimum O2 top up is £5, other networks £10

Anti-Surveillance Capitalism

- Once purchased, you can send the Top Up Voucher code number to some one else
 - Do not do this directly via SMS text message (unless encrypted)
 - Do not use plaintext unencrypted email for this
 - Embed the characteristic 12 or 19 digit etc. Voucher code in a longer message padded out with redundant data before encryption to confuse comms data traffic analysis.
- Instruct your confidential source not to immediately apply a Top Up Voucher code – they are usually valid for up to 6 months (N.B. Till printed paper vouchers often fade quite quickly)

Anti-Surveillance Capitalism

- Prepaid Mobile Phone Top Up Magnetic Stripe Swipe Cards
 - Some Networks e.g. EE or O2 allow you to register (via automated phone) a Magnetic Stripe Swipe Card with which to remotely top up mobile phone credit at a Supermarket checkout till etc.
 - Do not use
 - » Supermarket Loyalty Card
 - » Credit Card
 - » Contactless Payments
 - Do not Register (via phone) the Swipe Card at or near the physical location of a meeting with your confidential source.

Anti-Surveillance Capitalism

- Disposable “Burner” phones and Top Up Vouchers or Swipe Cards provided by journalists or activists to their sources can help to focus potential surveillance activities on themselves, rather than on the identities of their confidential sources,
- Some sources will be ok with getting their own, but they should be made aware of the risks.

Anti-Surveillance Capitalism

- Mobile Phone “Burner” handsets
 - Swapping SIM Cards does **not** cover your tracks
 - Call Detail Records include the International Mobile Equipment Identifier (IMEI) of the handset with every voice or data call or SMS text message
 - It is illegal in UK to re-program an IMEI (5 years in prison) or even to offer to do so !
 - Use cheap, prepaid Mobile Phone handsets £15 to £20 from Supermarkets etc., ideally not locked to one Network. - N.B. these stand out to GCHQ etc.
 - Use low end i.e. Android SmartPhones or better if you can afford them

Anti-Surveillance Capitalism

- Mobile Phone “Burner” handsets
 - See the previous slides about not drawing attention to yourself during a purchase
 - Opening the casing, removing the battery & inserting the SIM card etc. will leave lots of forensic evidence e.g. fingerprints, DNA samples, hair, fibre, dust etc. unless you take special care to avoid this e.g.
 - Ultraviolet light steriliser works by cross-linking DNA base pairs
 - kills bacteria & viruses & scrambles DNA “fingerprints”

Anti-Surveillance Capitalism

- Mobile Phone “Burner” handsets
 - Power on of a handset is location registered with the Network, **even without a SIM card inserted** (phones must offer 999 emergency calls even with no credit or contract)
 - First time use of a new SIM in a new handset is **specially tracked and recorded** (crypto keys are generated in the SIM card & sent to Mobile Network’s Home Location Register)

Anti-Surveillance Capitalism

- Mobile Phone “Burner” handsets
 - Do not activate your new handset and SIM card at home or where you meet your confidential contacts to hand over a “Burner” phone
 - You could try to mislead Communications Data snooping analysts by switching on your new mobile phone and SIM card in very busy locations e.g. close Railway Stations or Corporate HQs (but avoid CCTV)

Anti-Surveillance Capitalism

- Mobile Phone “Burner” handsets
 - Some mobile phone handsets can send an SMS message to a list of contacts when the SIM card is changed, as a security precaution against theft
 - Some mobile phone handsets can send an SMS message to a list of contacts when an Alarm key sequence is pressed – possibly useful in some arrest or physical attack scenarios
- Check if these features are enabled before swapping Mobile Phone handsets

Anti-Surveillance Capitalism

- What do GCHQ & other intelligence agency analysts do to track Burner Phones ?
 - <https://theintercept.com/2018/03/01/london-7-7-bombings-gchq-nsa-surveillance/>
 - <https://assets.documentcloud.org/documents/4390404/HIMR-Oct2011.pdf>

Anti-Surveillance Capitalism

GCHQ documents offer insight into another reason why the attackers may have managed to evade detection: At least three of them used cheap Nokia 1100 phones – probably “burner” devices that were not registered to them personally – and they communicated in what GCHQ called a “closed loop.” In other words, they only used their phones to talk to each other and did not make calls to anyone else, which appears to have thwarted the spy agency’s powerful surveillance apparatus.

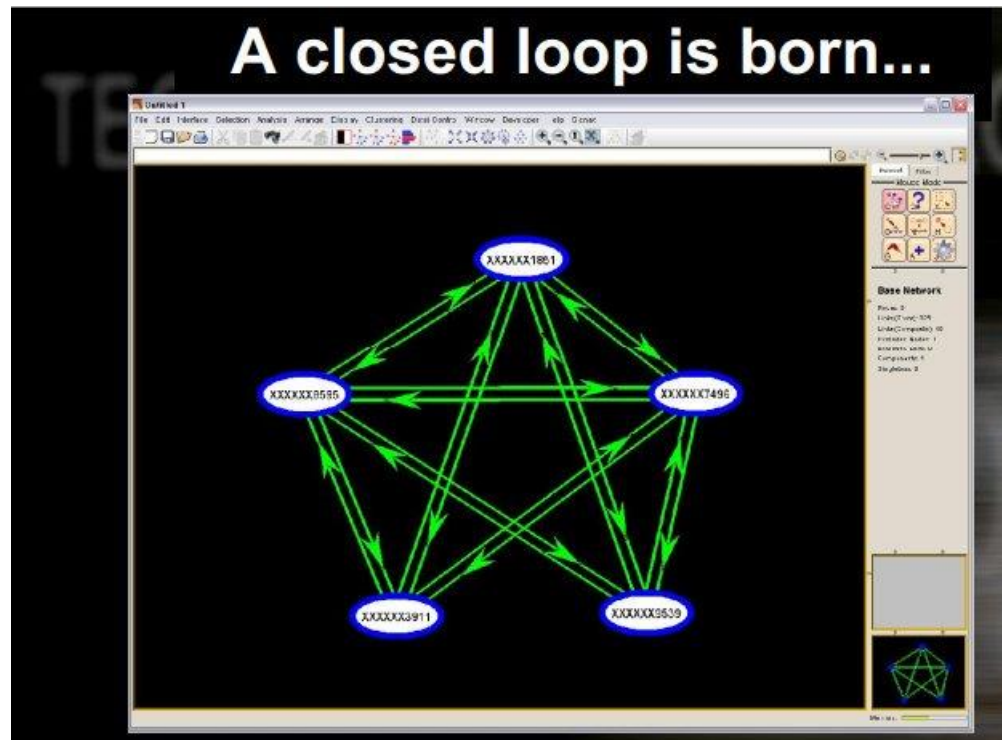
GCHQ later began specifically seeking out closed loops. In [an October 2011 document](#), the agency described how it had analyzed “anonymised metadata for bulk U.K.-U.K. mobile call records” in an effort to identify people who were communicating exclusively in small groups. They were a “rare phenomenon,” the agency concluded, but it added that among the few cases it did find, there were “possible target discovery opportunities.”

Anti-Surveillance Capitalism

The reality of target behaviour

- Targets from different IPT's regularly purchase groups of cheap mobile phones and use them operationally for a short period (possibly as long as three months) before getting a new set
- Two critical features:
 - Most of the phones start life at about the same time
 - Most of the phones are cheap handsets
- Sometimes the targets make a mistake and make a call to a phone outside the closed loop

Anti-Surveillance Capitalism



Anti-Surveillance Capitalism

The effect of windowing

- We need to window the data or else slip ups by the closed loop members will render the group invisible
- Need to choose a window that is large enough to allow the giant component to form but not so large that we never see targets who periodically goof up.

Anti-Surveillance Capitalism

- i.e. if Intelligence Agency or Surveillance Capitalism company analysts are looking too narrowly *only* for “Burner” phone Closed Loops, they may miss a group simply because of one or two calls outside of the group.
- Make a few calls to random private numbers or to unrelated public phone numbers to raise the cost of detailed analysis of your private communications.

Anti-Surveillance Capitalism

- Obviously with the resources of GCHQ, a Closed Loop of two or more Burner Phones is suspicious, but it is what e.g. a journalist and a whistleblower source need to maintain.
- If the discipline breaks down, even once and a call is made to a “normal” registered, traceable mobile phone or landline linked to you, then even Surveillance Capitalism companies like Google and Facebook will probably have all your details.

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - Do not contact multiple whistleblowers or confidential sources on the same identifiable phone
 - If one source is under investigation, then the others may **also** be compromised unnecessarily by the “mole hunt” for this source, through the “Friendship Tree” analysis of this phone.
 - Do not use “Burner” phones to contact any of your regular contacts at all – do **not** “phone home”

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - Word Codes for arranging meetings or document drops
 - Through other secure channels e.g. a face to face meeting, agree a simple Word Code to disguise Time & Location of meeting request / cancellation or document deliveries / pickups messages so that there is plausible deniability of the **content** of any voice calls or SMS texts

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - Beeping
 - Pre-arranged signals via mobile (or landline) phone without answering
 - » e.g. 3 rings and then hang up = “I am on the train, pick me up at the station in the next 15 minutes”
 - The Rules of Beeping: Exchanging Messages Via Intentional “Missed Calls” on Mobile Phones
 - <http://research.microsoft.com/apps/pubs/default.aspx?id=74532>

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - If you meet your confidential source face to face:
 - Ensure that you have switched off your identifiable mobile phone(s) (and 3G enabled Tablet computers or e-book readers) at least a kilometre away from the meeting location (in cities), at least 35 Km away in the countryside - or leave them switched **on** at home
 - Use a fresh pair of “Burner” phones for every meeting if you can afford this.

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - Even with “Burner” phones switch off:
 - Bluetooth (available on even cheap phones)
 - WiFi (usually only SmartPhones)
 - NFC (supposedly short range, but still a characteristic “fingerprint”)
 - GPS Location Services (mapping = tracking)
 - Aluminium kitchen foil Faraday Cage for devices where you cannot remove the battery e.g. Apple

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - Set a keyboard password / PIN on all your mobile phone handsets
 - This will not stop your Contacts and any SMS text messages or photos etc. from being forensically copied (or even Un-Deleted) if your phone is seized by the Police etc.
 - It will probably be enough to prevent the casual sort of snooping which police, security guards or family members etc. often engage in when they have access to your phone

Anti-Surveillance Capitalism

- Mobile Phone source protection tips
 - You can sometimes be tipped off to Direct Surveillance by unprofessional surveillance operatives using their Mobile Phones with Bluetooth wireless earpieces
 - It is worth scanning for Bluetooth devices when you are on public transport or in a pub or cafe etc. for a meeting to see if any familiar or suspicious Bluetooth devices are nearby

Anti-Surveillance Capitalism

- Webmail & Social Media accounts
 - CryptoParty London is an opportunity to swap:
 - “free” web email accounts e.g. gmail or yahoo
 - “free” social media accounts e.g. Twitter or FaceBook
 - “free” public WiFi credentials (if you use a VPN)
 - Investigative journalists & bloggers etc. should always have a few “free” accounts ready to hand, in case they are contacted by whistleblowers

Anti-Surveillance Capitalism

- Webmail & Social Media accounts
 - Pick a plausible name not an obvious pseudonym e.g. “Charles Farr” rather than “Mickey Mouse”
 - Go through the normal free web based registration process
 - Use Google Maps to find plausible real addresses and post codes, ideally in multi-tenant buildings in busy cities e.g. Buckingham Palace London SW1A 1AA

Anti-Surveillance Capitalism

- Webmail & Social Media accounts
 - Use the Tor software which you have learned about at the CryptoParty London or with which you are already familiar
 - If Two Factor Authentication is required e.g. for Google or Twitter use your the disposable “Burner” mobile phone number
 - use the full international dial code if you are in physically different country to that where you are apparently registering from
 - e.g. +44 (0)794 366 1808

Anti-Surveillance Capitalism

- Webmail & Social Media accounts
 - Some web account registrations only check that a phone number has the correct number of digits and do not attempt to dial it or send an SMS text.
 - Make a note of the Username and initial Password of the account(s) you have created
 - Bring these along to the next CryptoParty London or similar event and swap them with ones created by other attendees

Anti-Surveillance Capitalism

- Webmail & Social Media accounts
 - Remember that provided you do not intend to commit fraud, you are legally entitled to use any name(s) or pseudonym(s) or aliases you wish, in the United Kingdom.
 - Mrs. Cherie Blair is also legally known as Ms. Cherie Booth QC

Anti-Surveillance Capitalism

- Webmail & Social Media accounts
 - When you get away from the CryptoParty London, log in to your newly acquired web email or social media accounts, ideally using Tor or other VPN proxy techniques
 - Change the password and bump up the privacy settings e.g. turn on “always use https:// SSL connections” if possible
 - N.B. some free accounts expire quickly if not used e.g. after 3 weeks of inactivity for free encrypted Hushmail.com email accounts

Anti-Surveillance Capitalism

- N.B. you can arrange to create and securely swap social media or email accounts or mobile phone credit vouchers etc. in the future, provided you have established some trust and a communications channel here, face to face.
- Questions ?
- Now let's see what you have brought to swap or barter ...