

CryptoParty London 3  
12th December 2012

# CryptoParty Bring & Swap

- CryptoParty London Bring & Swap
  - 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
  - Webmail & Social Media accounts

# CryptoParty Bring & Swap

- Avoid drawing attention to yourself as you make a purchase
  - Use Cash
  - No Credit Cards
  - No Cheques
  - No Supermarket Loyalty Cards e.g. Nectar

# CryptoParty Bring & Swap

- 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.

# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- 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.

# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- 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” !





# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- Oyster Card
  - Oyster Card (and 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.

# CryptoParty Bring & Swap

- 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 by the Conservative / Lib Dem Coalition Home Secretary Theresa May.
  - Ministerial Certificate signed 4th July 2007:  
[DPA/s.28/MPS/2007/CC1](#)

# CryptoParty Bring & Swap

- Oyster Card
  - 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

# CryptoParty Bring & Swap

- Oyster Card Swap:
  - 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
    - Swap for another unused Oyster Card
  - Do not buy or register the Oyster Card online

# CryptoParty Bring & Swap

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

# CryptoParty Bring & Swap

## – Mobile Phone Swaps

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

# CryptoParty Bring & Swap

- 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



# CryptoParty Bring & Swap

- Prepaid Mobile Phone Credit Top Up Vouchers
  - Do not use
    - » Supermarket Loyalty Card
    - » Credit Card
    - » 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 T-Mobile top up is £5, other networks £10
- Once purchased, you can send the Top Up Voucher code number to some one else
  - Do not do this directly via SMS text message
  - Do not use unencrypted email for this

# CryptoParty Bring & Swap

- Prepaid Mobile Phone Top Up Mag Stripe Swipe Cards
  - Some Networks e.g. Orange or T-Mobile allow you to register 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
- Useful for investigative journalists etc. who have given a “burner” mobile phone to a whistleblower or confidential source

# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- 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)
  - 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)
  - Do not do this at home or where you meet your confidential contacts.

# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- Do not contact multiple whistleblowers or confidential sources on the same phone
  - If one source is under investigation, then the others may also be compromised unnecessarily by the “mole hunt”

# CryptoParty Bring & Swap

- 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
  - Investigative journalists & bloggers etc. should always have a few “free” accounts ready to hand, in case they are contacted by whistleblowers



# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- Webmail & Social Media accounts
  - Use the Tor software which you have learned about at the CryptoParty 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

# CryptoParty Bring & Swap

- Webmail & Social Media accounts
  - Many 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 and swap them with similar ones created by other attendees

# CryptoParty Bring & Swap

- 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

# CryptoParty Bring & Swap

- Webmail & Social Media accounts
  - When you get away from the CryptoParty, 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

# CryptoParty Bring & Swap

- Questions or corrections to Mark at:
- Web: <https://CryptoParty.org/wiki/London>
- Twitter: [@CryptoPartyLond](https://twitter.com/CryptoPartyLond)
- Email: [info@CryptoParty.org.uk](mailto:info@CryptoParty.org.uk)
- PGP Key ID: [0x8997f1b8](#)