CryptoParty London
29th Sept 2012

UK Legal Aspects of Cryptography & Anonymity

- Who can legally snoop on your communications etc. ?
- National Security
  - Espionage
  - Terrorism
  - Economic well being of the United Kingdom
- Serious Organised Crime investigations
  - » Drug Smuggling
  - » Human Trafficking
  - » Counterfeit Goods

UK Legal Aspects of Cryptography & Anonymity

- Who can legally snoop on your electronic communications etc. ?
  - General low level crime
  - Criminal investigations no longer handled by the Police
    - Her Majesty's Revenue & Customs (HMRC)
    - Department for Work & Pensions (DWP)
    - Local Authority Trading Standards
    - Local Authority Environmental Health
    - Anti-fraud Private Investigators & Insurance Co's

UK Legal Aspects of Cryptography & Anonymity

- Who can legally snoop on your electronic communications etc. ?
  - General low level crime
  - Criminal investigations no longer handled by the Police
    - Her Majesty's Revenue & Customs (HMRC)
    - Department for Work & Pensions (DWP)
    - Local Authority Trading Standards
    - Local Authority Environmental Health
    - Anti-fraud Private Investigators & Insurance Co's

UK Legal Aspects of Cryptography & Anonymity

- Who can legally snoop on your electronic communications etc. ?
- Civil Law – Court Orders involving
  - Copyright Infringement
  - Libel

UK Legal Aspects of Cryptography & Anonymity

- Almost every other civilised country in the world requires some form of independent Judicial Warrant to snoop on
  - the Content of your communications
  - the Communications Data generated by such communications
- But no Judicial Warrants are allowed in the United Kingdom!

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 (“RIPA”) – very complicated
  - http://www.legislation.gov.uk/ukpga/2000/23/contents
  - Part I Chapter I Interception (of electronic and postal communications)
  - Self authorised warrants submitted by the Police & Intelligence Agencies, rubberstamped by Home Secretary or Foreign Secretary or their “Sir Humphrey” proxies

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part I Chapter I – unnecessary secrecy
  - UK Intercept evidence cannot be used in Court, but Foreign Intercept evidence can be
  - up to 2 years in prison for illegal interception
  - but up to 5 years in prison “tipping off” offence for revealing the mere existence of an Intercept Warrant, no exceptions

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part I Chapter I
  - Definition of electronic communications
    - Covers the entire electromagnetic spectrum !
    - Covers everywhere in the UK and everywhere outside UK i.e. the entire universe !
  - Legally conducted by MI5, MI6, Police units who get the Telcos & ISPs & Post Office to do the actual work

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part I Chapter I
  - Only GCHQ should have its own legal physical interception capacity
  - Legal grey area for UK Military units who have e.g. airborne electronic warfare intercept equipment
  - Legal grey area for Police etc. using IMSI catchers e.g. Harris Corp. Stingray
- **Protect your communications from abuse by overzealous or corrupt bureaucrats with Cryptography e.g. PGP**

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part I Chapter II Acquisition and disclosure of communications data
  - Again, no Judicial Warrant required at all
  - Self Authorisation by Police, Intelligence Agencies, other Government Departments & Agencies and 650 Local Authorities etc.
  - No external authorisation of Data Protection Act section 29 demands, but most now use a trained Single Point of Contact team

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part I Chapter II – Communications Data
  - Works in tandem with European Union Data Retention Regulations (proposed by UK !)
    - Mandatory retention of innocent users phone records for 1 year
    - Mandatory retention of innocent users UK ISP based email logs for 1 year
    - Most investigations actually only need current or very recent data. e.g. last week

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part II – Communications Data
  - **No criminal penalties for abuse of Communications Data** e.g. selling to tabloids or private investigators
  - UK law is already much more intrusive than the recent legislation in Australia which helped to spark off the CryptoParty meme

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part II – Communications Data
  - A detailed “Friendship Tree” of who communicated with whom, when and where can be more intrusive than the interception of the often bland, content of communications
  - Mobile Phone device Location Based Services Communications Data is valuable commercially and potentially very intrusive.
- **Protect the Anonymity of your communications with e.g. Tor**

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part III Investigation of electronic data protected by encryption etc.
  - Section 49 Notices self authorised by “a Police constable” demanding either
    - De-cryption Keys
    - De-crypted plain text
  - Can also be ordered by a Court

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part III Investigation of electronic data protected by encryption etc.
  - Failure to comply with Section 49 Notice
    - Up to 2 years in prison
    - Up to 5 years in prison if the words “National Security” or “Child Indecency” are invoked
  - Up to 5 years in prison for “tipping off” if the Secrecy provision is invoked
  - Ignored by serious criminals & terrorists who face longer prison sentences anyway

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part III Investigation of electronic data protected by encryption etc.
  - "Reverse Burden of Proof"
    - You have to try to prove a negative, that you do not / did not have access to the De-cryption keys or the plain text
  - But there is an "I've genuinely forgotten my PGP passphrase" defence
    - Not viable for Whole Disk Encryption of a computer provably in use recently

UK Legal Aspects of Cryptography & Anonymity

- Regulation of Investigatory Powers Act 2000 Part III Investigation of electronic data protected by encryption etc.
  - On the Statute Book for 7 years before it was Commenced
  - No recorded “National Security” use of this power, ever.
- **Protect the confidentiality of your data with Cryptographic tools e.g. PGP or TrueCrypt**

UK Legal Aspects of Cryptography & Anonymity

- Draft Communications Data Bill
  - Currently being mulled over by a Joint Committee of Parliament
  - http://wiki.openrightsgroup.org/wiki/Communications_Data_Bill/Draft
  - Proposals to extend the RIPA and Data Retention schemes way beyond phones and email etc. to use Deep Packet Inspection to snoop on web search engines, Voice over IP, internet chat, online multi-player games etc.

UK Legal Aspects of Cryptography & Anonymity

- Draft Communications Data Bill
  - http://www.parliament.uk/documents/joint-committees/communications-data/Communications%20Data%20formatted%20written%20evidence.pdf
    - Serious Organised Crime Agency (SOCA) evidence Annex page 373 ff gives a Scenario to illustrate modern day (innocent !) digital life.
    - They want to be able to snoop on all of this, in secret, without a Court Order or Judicial Warrant.

UK Legal Aspects of Cryptography & Anonymity

- Draft Communications Data Bill
  - Multi-billion £ plans for Deep Packet Inspection automated “filters”, man-in-the-middle attacks on http**s**:// secure websites etc., especially if hosted overseas
  - Serious Criminals and Terrorists etc. are already evading such plans.
  - No technical details yet, but these vague plans can only be legally circumvented using CryptoParty basic tools and techniques.

UK Legal Aspects of Cryptography & Anonymity

- Electronic Communications Act 2000
  - http://www.legislation.gov.uk//ukpga/2000/7
    - Licensing scheme for commercial Cryptographic Services e.g. Trusted Third Party Key Escrow
      - Almost nobody uses these in the UK
    - Digital Signatures are legally binding in UK for contracts etc., if all / both parties agree
      - Unlike other countries this is not specifically for Cryptographic Hashed Digital Signatures
      - Any email .sig file / plaintext / graphic "signature" will do

UK Legal Aspects of Cryptography & Anonymity

- Electronic Communications Act 2000
  - Digital Signatures could technically provide the cunning concept of Non-Repudiation
  - So far, there are no test cases which have established legal precedents which uphold this concept in the UK

UK Legal Aspects of Cryptography & Anonymity

- Electronic Communications Act 2000
  - Activists should use Digital Signatures e.g. PGP / GPG, for Press Releases, calls for public meetings etc.
    - Fake public meetings called during “Arab Spring”
  - Everyone should verify the authenticity of PGP signed emails about Software Security Vulnerabilities e.g. from Microsoft or from GovCertUK etc.

UK Legal Aspects of Cryptography & Anonymity

- Data Protection Act 1998
  - http://www.legislation.gov.uk/ukpga/1998/29/schedule/1
- 7th Principle of Data Protection = Crypto
  - "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

UK Legal Aspects of Cryptography & Anonymity

- Public Officials hide behind Anonymity e.g. when (not) fully answering your Freedom of Information Act 2000 requests
- Anonymity for individual members of the public is under constant attack
- No Anonymity guarantees for whistleblowers under the Public Interest Disclosure Act 1998

UK Legal Aspects of Cryptography & Anonymity

- The forthcoming Defamation Bill 2012
  - some welcome Libel reforms
  - but Clause 5 Operators of websites targets Anonymous blog & chat forum comments
    - Twitter etc. can afford expensive legal costs,
    - Individual blog operators cannot afford to be forced to go to court to defend themselves
      - They will be shut down by Lawyers' demands to identify anonymous blog comment posters
- Use Tor etc. to hide your IP address when posting Blog Comments or Tweets

UK Legal Aspects of Cryptography & Anonymity

- Force the UK public & private sectors to use strong Cryptography to protect your data
- Call for resignations or prosecutions for misfeasance in public office or professional negligence or if unencrypted personal data is lost or stolen e.g.
  - 25 million child benefit records by HMRC
  - , 1 million military recruitment records

UK Legal Aspects of Cryptography & Anonymity

- **If you don't like the law, get it changed !**
- Support these cross party campaign groups e.g.
  - NO2ID Campaign
    - NO2ID.net
  - Open Rights Group
    - OpenRightsGroup.org
  - Liberty Human Rights
    - www.liberty-human-rights.org.uk

UK Legal Aspects of Cryptography & Anonymity

- Lobby your elected representatives:
  - Local Councillors
  - Greater London Assembly Members
  - Members of Parliament (MP)
  - Members of the European Parliament (MEP)
- Check on what your MP has said on the topics of privacy & security & liberty
  - www.theyworkforyou.com
- Find & Email / Fax your elected politicians
  - www.writetothem.com

CryptoParty London

- Questions or corrections to Mark at:

- Web: https://CryptoParty.org/wiki/London
- Twitter: @CryptoPartyLond
- Email: info@CryptoParty.org.uk
- PGP Key ID: 0x8997f1b8