Internet Anonymity with Mobility
Key Challenges for the Future

Stephen Doswell
Graduate Tutor
Faculty of Engineering and Environment
May 2013

My Profile

- Graduate Tutor – also PhD research student:
  - Just completed 1st year of research
  - Supervisors: Dr Nauman Aslam, Dr David Kendall, and Dr Graham Sexton;

- Academic background: MSc Digital Forensics, BSc Computing and Psychology;

- Teach on two Ethical Hacking modules and supervise 4 final year BSc projects;

- 15 years commercial experience.

Context within Society - Privacy

Right to Privacy

- **Privacy** is a human right;
- Privacy of **correspondence (communications)** is outlined by:
  - **Article 12** of the United Nations Universal Declaration of Human Rights (1948);
  - **Article 8** of European Convention of Human Rights (1953);
  - **Human Rights Act (1998)** within **United Kingdom** law.

Challenges to Privacy

- A right to privacy of communications except: "

…in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

- **Regulation of Investigatory Powers Act (RIPA) 2000**
  - Requires a court order based on sufficient evidence and/or intelligence for law enforcement and/or security agencies of the UK Government to undertake surveillance of a **named** individual's mobile phone records, e-mails, Internet activity etc. **RIPA currently under review**.

Challenges to Privacy (Update)

- **Communications Data Bill 2012**

Proposed that a court warrant, evidence and/or intelligence are **no longer required** by law enforcement and security agencies of the UK Government, who undertake real-time surveillance of **all** citizen's mobile phone records, e-mails, Internet activity etc.; regardless of any suspicion or otherwise.

The balance between a providing a right to privacy of communications and at the same time maintaining national security and prevention of crime, is a long running debate, not just in the United Kingdom but across the world.

Challenges to Privacy (Latest Updates)

- **Communications Data Bill –** not included during Queen's speech (May 2013);

- Proposed 'review' (possibly even repeal) of the **Human Rights Act 1998**, possibly replaced by a UK 'Bill of Rights';

'Bill of Rights' - will the right to privacy of communications be included, and if so, to what extent?

A continually changing position…!

Privacy Enhancing Technologies (PETs)

Privacy Enhancing Technologies

- **Privacy Enhancing Technologies (PETs)** covers a wide range of tools and techniques with the aim to protect an individual's privacy within technological environments, including:

  - Cryptography – e.g. disk encryption, encrypted network traffic;
  - Steganography – e.g. hiding 'sensitive' documents within photographs;
  - Obfuscation – e.g. morphing Peer-to-Peer (P2P) traffic into Voice over IP (VOIP) to by-pass blocking, improve network priority;
  - **Pseudo-identity** – Proxy services, Virtual Private Network (VPN), and Anonymous Communication Systems (**Anonymity Networks**);
  - Anti-forensics, counter-surveillance;

Anonymity Networks

- Anonymity networks, such as '**The Onion Router'** (officially known as **Tor** not TOR), aim to provide a degree of anonymity for an individual's Internet traffic;

- Tor uses a technique known as **Onion Routing**, which is based on the original theory of **Mix-nets**;

- The Tor network is free to use, and can be accessed from a range of software (e.g. Tor Browser Bundle (TBB)) and is available on a number of platforms / operating systems.

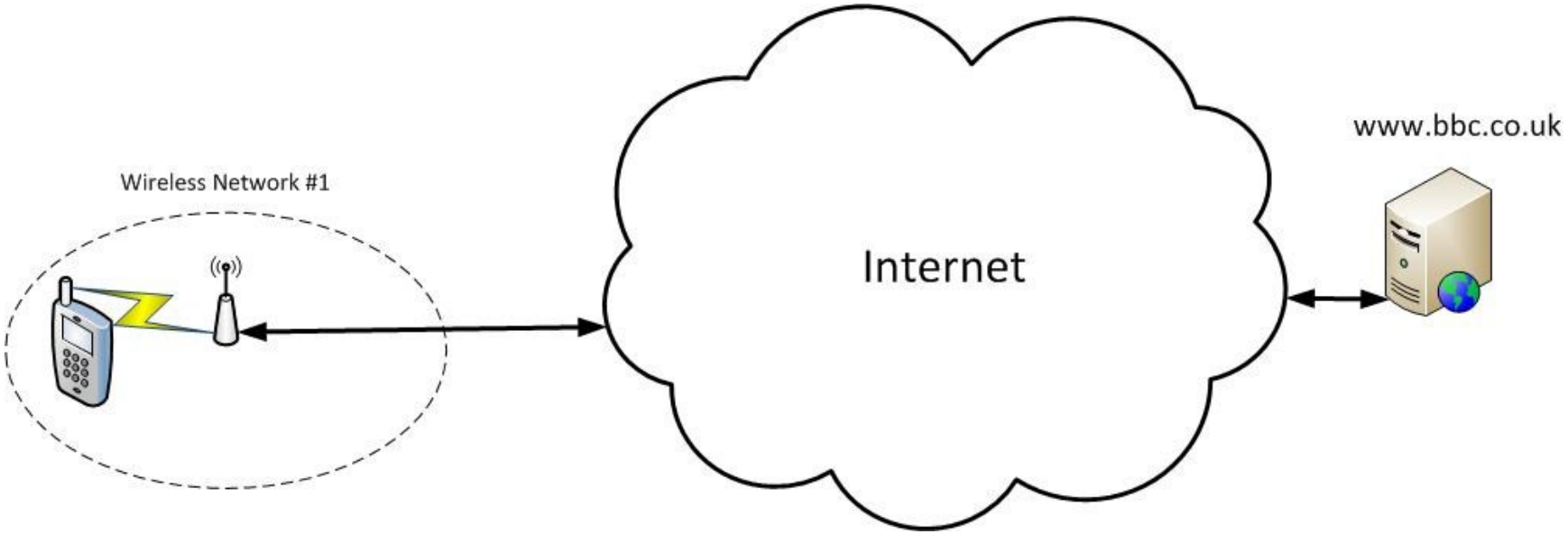
Tor – How does it work?

- The Tor network is a **distributed overlay network** which sits ‘on top’ of the Internet itself, and uses the standard Internet Protocol (IP) for network routing;

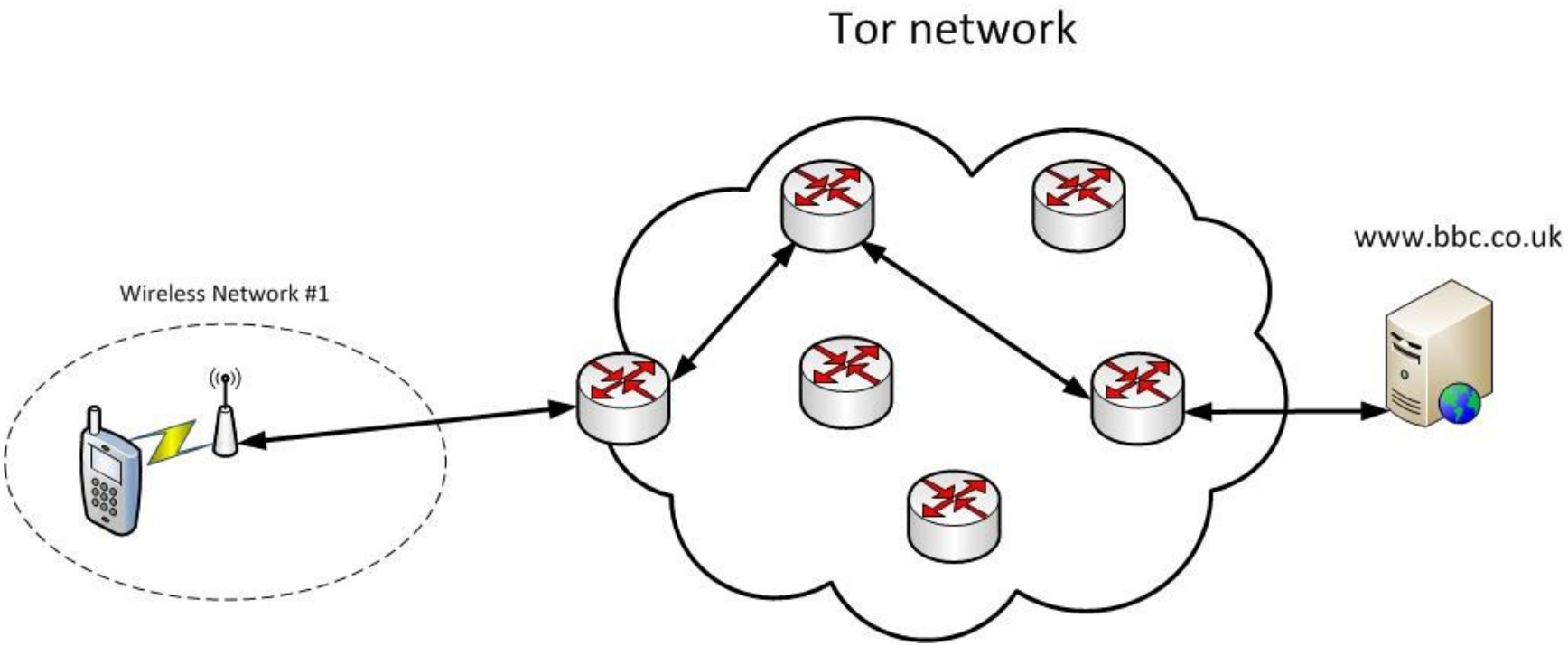
- Acts as a **multi-hop proxy** between a Tor client and the destination e.g. website; combined with **cryptography** in order to provide anonymous web-surfing and privacy;

- Tor uses Transmission Control Protocol (TCP) as it’s transport protocol, however as an overlay network, Tor additionally requires application level congestion control to try and ensure steady traffic flow within the anonymity network itself.

The Internet (simple version!)



The Tor Network (another simple version!)



Key statistics as at 13/05/2013:

3500 routers worldwide relaying Internet traffic;
1700 bridges to the Tor network to circumvent the blocking of accessing the Tor network;
Average of **500,000 – 600,000** daily users;

Source: https://metrics.torproject.org/

Key ‘Privacy-Enhancing’ Features of Tor

- The **3-hop approach** ensures that no Tor router has a complete view of the circuit; as each layer is only revealed one ‘hop’ at a time, which contains the IP address of the next destination and remaining layer;

- **Cryptography**, in terms of both circuit creation (‘telescoping’) and also applied to each layer of the message using Transport Layer Security (TLS) e.g. as with HTTPS for on-line banking etc.;

- The **session keys** used for the cryptography are **ephemeral (short-lived)**, which reduces the risk of a ‘replay’ attack.

Research Problem

Anonymity with Mobility

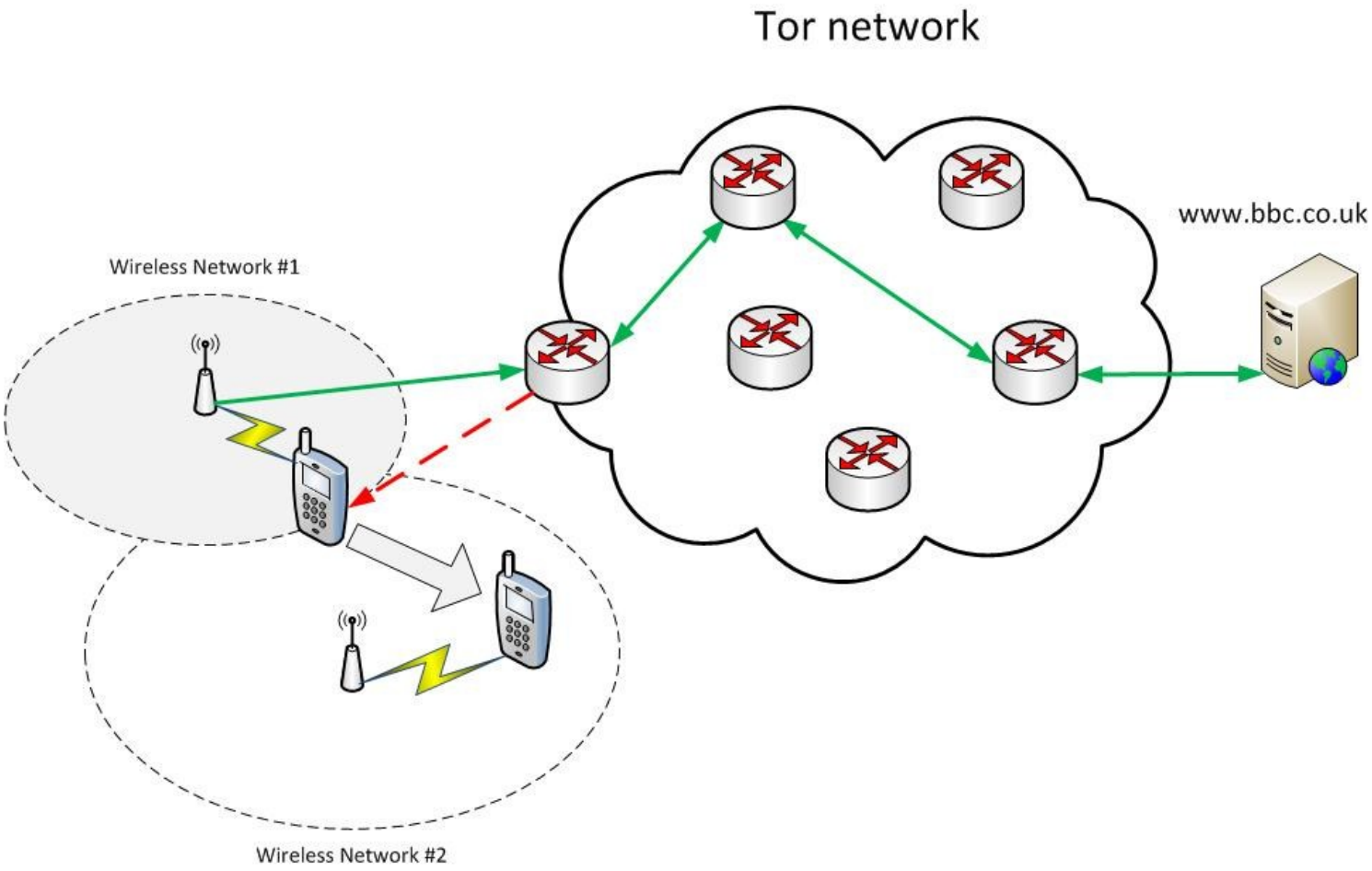
- **Estimates are that Internet connections from mobile devices are expected to exceed connections from 'static' by 2014:**
  - Latest estimates towards the end-2013;
  - Some places have already achieved this e.g. South Korea.

- **Since 2010, Tor available on 'smart' phone technology as Orbot for Android:**
  - Initially a joint development project from Google and University of Cambridge but now maintained by The Guardian Project;
  - Limited research so far has been undertaken to assess the performance for mobile Tor clients and the two studies have not looked at the implications of 'roaming' between networks.

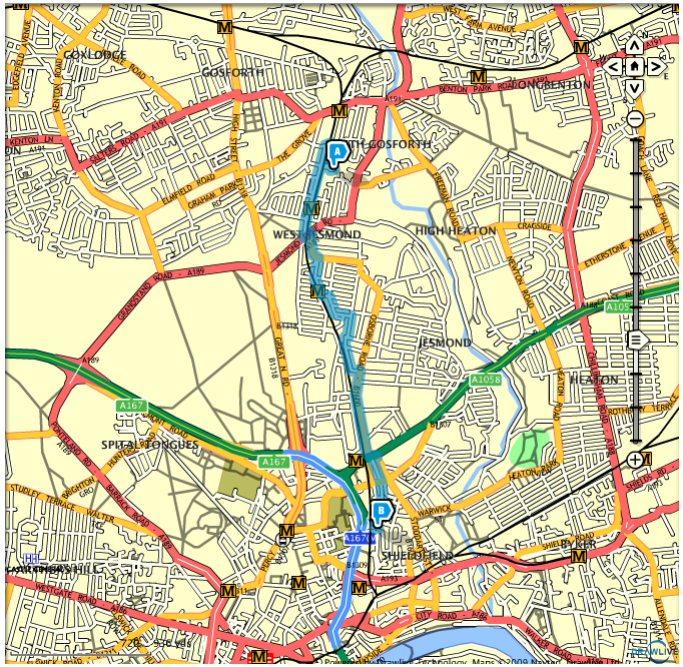
Key issues

- Onion Routing (1996) and Tor (2004) were designed at a time when only static devices accessed the Internet. The current design requires the client to have a **persistent Internet connection (incl. external IP address)**, to maintain circuit integrity;
- Tor currently takes an average of over **7 seconds to rebuild circuits** for a new Internet connection;
- '**Roaming**' between networks (or even within same service e.g. BT Wifi™) may change a Tor mobile client's external IP address every couple of minutes while walking – or even more if 'commuting'.

Key issues (2)


Tor network
www.bbc.co.uk
Wireless Network #1
Wireless Network #2

Case Study



My daily walk to work:

Start @ A:

- Hutchinson 3 Wi-Fi

En-route:

- 6 x BT Wi-Fi hand-offs;

- ‘Black spot’ @ Jesmond Dene Road revert to EE cellular *(Expensive!);*

- 7 x BT Wi-Fi hand-offs;

Finish @ B:

-Northumbria University Wi-Fi *(Free!)*

Total: 4 different services, 15 hand-offs.

Early modelling

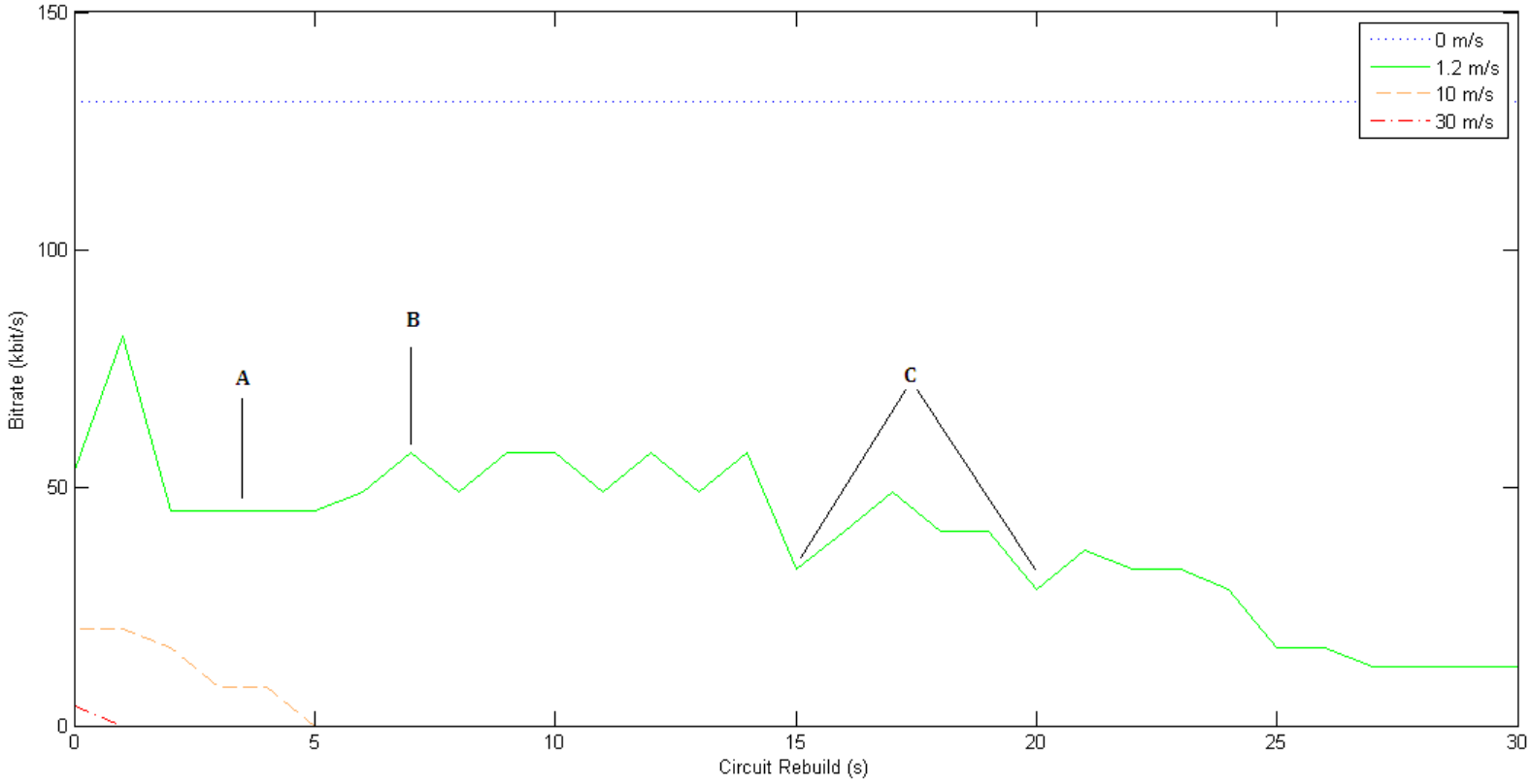
Aim:

- Assess the potential impact to both the mobile client and overall Tor network, using Tor while roaming;

Approach:

- Undertake initial modelling through network simulation tools (OMNET++), Matlab, and laboratory experiments;
- Simulate a mobile Tor client roaming between networks at different speeds (m/s) and introduced circuit rebuild timings (s); with differing web browsing loads.

Early modelling results



Key points:

1. At higher speeds (commute - bus, highway – car), the use of Tor is not feasible;
2. Even at average walking pace of 1.2 m/s, a significant (66% – 77%) drop in performance; indicative markers at A (3), B (7), C (15 to 20) seconds, as timings for `good', `average' and `slow' circuit build times respectively
3. An average of 3 - 4% ‘orphaned’ data observed left by the mobile Tor client after hand-off; which causes additional congestion within the wider Tor network; due to two-tier traffic management.

Contribution

Possible solutions

- '**Architectural**' **changes** to how Onion Routing and Tor works, with the aim to provide a **persistent connection to the Tor network** even when a mobile Internet connection is broken. *University of Wollongong examined and rejected the use of **MobileIP***;

- '**Lighter**' **transport protocols** to replace TCP, such as UDP-based 'fire-and-forget'. *The University of Cambridge are currently testing Tor with **µTP***;

- '**Throttling**' mobile Tor clients, to assess **risk of** and/or **predict** hand-off; and adapt the amount of traffic entering the Tor network accordingly to reduce potential congestion. *University of Waterloo researching 'throttling' for Tor clients using Peer-to-Peer*.

Current work

April - June 2013:

Analysis (modelling) of different application-level throttling algorithms, based on previous work by University of Waterloo to throttle Bit-torrent users on Tor; and evaluate effectiveness for mobile scenarios;

Aim to ‘optimise’ the balance between performance for the mobile client and impact on the Tor network;

Results and findings expected **end-June**.

Current and future challenges / drivers

- The current lack of suitable simulation tools, in terms of accurately simulating both mobility and Tor together;
- The impact on this research if Tor adopts new lighter transport protocol e.g. µTP – less congestion?;
- Development (sponsored - $1m) of Tor-supported Voice-over-IP (VoIP) tool - more mobile (and persistent) Tor usage?;
- Increased migration to HTML5 support (e.g. Youtube); to reduce the requirement of `unsafe' Flash player – more streaming, live and/or recorded traffic over Tor?

Warning

The use of Privacy Enhancing Technologies (PETs) is **illegal** in some countries.

For example, in one country, the tariff for attempting to circumvent government censorship and/or restrictions, using Tor etc., is **15 years** imprisonment.

Please ensure that you are aware of your local laws before attempting to use any PETs.

Thank you.

Any Questions?