

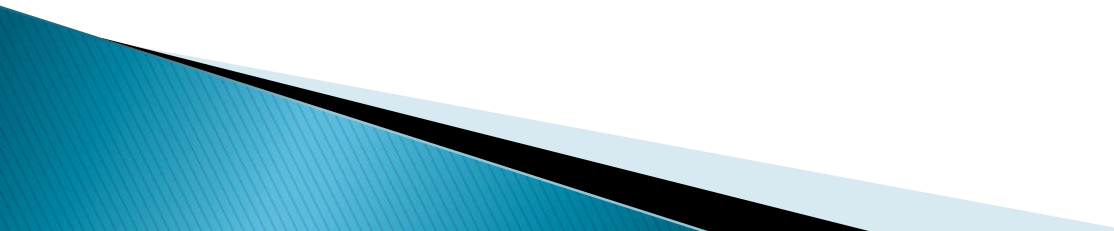
PRIVACY MATTERS

Yes it really does....

The Investigatory Powers Act 2016

- ▶ Nicknamed the *Snoopers' Charter*
- ▶ Something everyone who uses the Internet in this country ought to know about

The Investigatory Powers Act 2016

- ▶ This new law forces telecommunications companies to retain comprehensive personal data records of all of their customers (websites visited and phone numbers called) for a period of 12 months. This then may be made available to a huge range of bodies without telling you and without a warrant:
- 

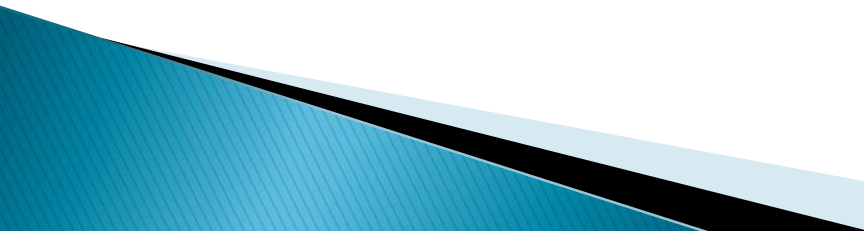
The Investigatory Powers Act 2016

- ▶ Metropolitan Police Service
- ▶ City of London Police
- ▶ Police forces maintained under section 2 of the Police Act 1996
- ▶ Police Service of Scotland
- ▶ Police Service of Northern Ireland
- ▶ British Transport Police
- ▶ Ministry of Defence Police
- ▶ Royal Navy Police
- ▶ Royal Military Police
- ▶ Royal Air Force Police
- ▶ Security Service
- ▶ Secret Intelligence Service
- ▶ GCHQ
- ▶ Ministry of Defence
- ▶ Department of Health
- ▶ Home Office
- ▶ Ministry of Justice
- ▶ National Crime Agency
- ▶ HM Revenue & Customs
- ▶ Department for Transport
- ▶ Department for Work and Pensions
- ▶ NHS trusts and foundation trusts in England that provide ambulance services
- ▶ NHS National Services Scotland
- ▶ Competition and Markets Authority

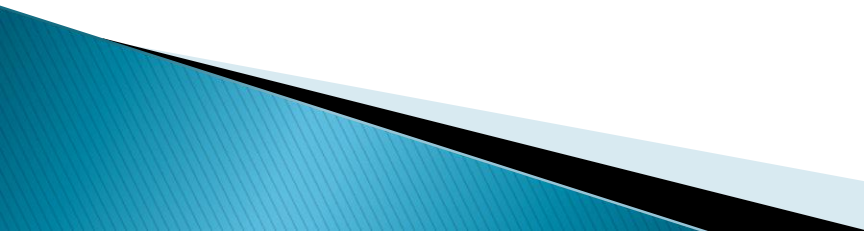
The Investigatory Powers Act 2016

- ▶ Criminal Cases Review Commission
- ▶ Department for Communities
- ▶ Department for the Economy
- ▶ Department of Justice (Northern Ireland)
- ▶ Financial Conduct Authority
- ▶ Fire and rescue authorities under the Fire and Rescue Services Act 2004
- ▶ Food Standards Agency
- ▶ Food Standards Scotland
- ▶ Gambling Commission
- ▶ Gangmasters and Labour Abuse Authority
- ▶ Health and Safety Executive
- ▶ Independent Police Complaints Commission
- ▶ Information Commissioner
- ▶ NHS Business Services Authority
- ▶ Northern Ireland Ambulance Service
- ▶ Northern Ireland Fire and Rescue Service Board
- ▶ Health & Social Care Business Services Organisation
- ▶ Office of Communications
- ▶ Police Ombudsman for Northern Ireland
- ▶ Police Investigations and Review Commissioner
- ▶ Scottish Ambulance Service Board
- ▶ Scottish Criminal Cases Review Commission
- ▶ Serious Fraud Office
- ▶ Welsh Ambulance Services National Health Service Trust

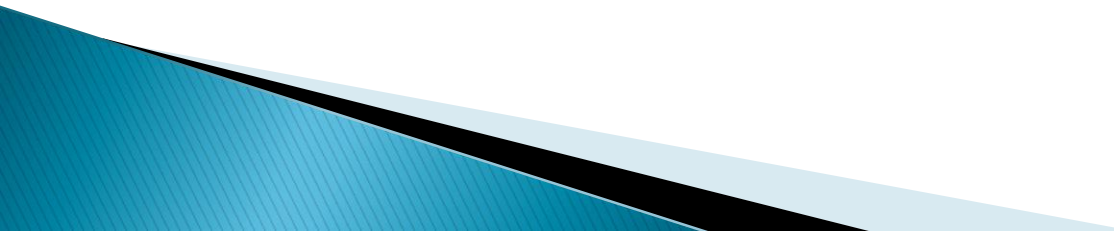
The Investigatory Powers Act 2016

- ▶ Many people are deeply unhappy about this
 - ▶ It is in force now – though in December 2016, the European Court of Justice declared that general surveillance on a mass scale is unlawful and there may yet be legal challenges to it
 - ▶ It is the most far-reaching such law in Europe and it is similar to the laws in China and Russia
- 

The Investigatory Powers Act 2016

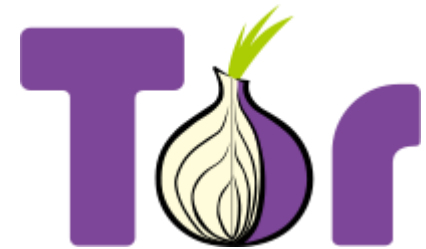
- ▶ ISP's must comply with it – though we do not know if any have yet because they are not allowed to tell us that they are doing it
 - ▶ It will start with the bigger companies (BT TalkTalk etc)
 - ▶ It may never happen with the smallest companies
 - ▶ You may take the 'I have nothing to hide' position – but it is something we all need to be aware of
- 

The Investigatory Powers Act 2016

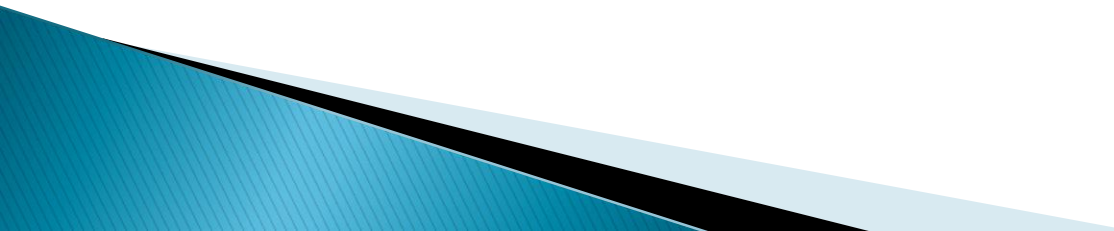
- ▶ What can we do about it?
 - ▶ Not much – just be aware that it may be happening
 - ▶ You could get round it by using a service which does not log your usage
 - ▶ That may be too technically challenging for many people, but here is a suggestion:
- 

The Investigatory Powers Act 2016

- ▶ To be anonymous on the Internet you can use TOR – ‘The Onion Router’ – which makes what you do untraceable
- ▶ It is widely used for quite legal (and some illegal) purposes. It’s use is common in ‘Internet-censoring’ countries such as China, Russia and places where you are tracked – like the UK!



Privacy – protect yourself online

- ▶ Not just about privacy but also about protection from criminal activity
 - ▶ You don't want to be an easy target for 'Identity Theft'
 - ▶ Do not put online any information which will easily identify you or make the criminal's job easier
 - ▶ Remember - The Internet is a 'public place'
- 



- ▶ Don't reveal your full name
- ▶ Lie about your date of birth (but keep a record of what you used)
- ▶ Don't add any details which might help a fraudster (schools attended; work places etc)
- ▶ Don't reveal any address details – including the town



- ▶ Be vague about family members (e.g. ‘my daughter’ rather than naming her perhaps)
- ▶ Don’t accept as ‘friends’ anyone you don’t actually know offline
- ▶ Don’t allow ‘friends of friends’ to add themselves
- ▶ Don’t automatically accept friend suggestions (FB gives me a possible list of 140 people!)
- ▶ Don’t post your ‘phone number



- ▶ Make full use of the security and restriction settings
- ▶ Don't post photos of the inside of your home (*burglars love that...*)
- ▶ Don't post your holiday dates (*...they love that too!*)
- ▶ Be very careful what you post – even following the above guidelines it still may be possible to find out a lot about you from your posts

...and

- ▶ Similar advice applies to all Social Media sites



- ▶ ... records every site you visit of course (as do most other 'search engines' – including Yahoo; MSN and Bing)
- ▶ You can clear Google's records if you have a Google account
 - ▶ *Search for 'Delete searches & other activity from your account'*
You can also tell Google to stop saving your activity altogether if you want

Your Computer

- ▶also stores a list of every website you visit and data from each site
- ▶ This is not kept ‘forever’ but it is kept for a long time
- ▶ You CAN delete your browsing history from your browser – Internet Explorer; Chrome; Firefox; Edge
 - ▶ In *Internet Explorer* use *Ctrl+Shift+Delete*
(*this works in other browsers too*)

Your Computer

- ▶ You should think carefully about allowing your browser to store passwords (if they are stored on your computer then anyone using it can find them and a hacker can readily get them using malware – another reason to have good and up to date anti-virus software)
- ▶ To find what is stored is easy:
 - ▶ For example in Firefox *Click Tools>Options on the main Firefox menu. On the Options page click Security>Saved Logins. Then click Show Passwords.*

Public Wifi

- ▶ You should be very careful using public wifi.
- ▶ There may be little security to stop someone intercepting the information you enter (e.g. banking or other personal information, passwords and user names)

General Help

- ▶ There is an excellent national website well worth looking at
 - ▶ It is a mine of information and advice
 - ▶ <https://www.getsafeonline.org/>
- 