

Investigatory Powers Act

Philip and Mo

It's official, the Snooper's Charter is becoming law: how the IP Bill will affect you

The Investigatory Powers Bill has been passed by both Houses of Parliament. Once it receives Royal Assent it will become law

The Act

- Proposed first in 2013 by Theresa May as Home Secretary
- Re-proposed, and taken into Law in 2016.
- Claimed by the government to put restrictions on the ability of institutions to see private data.
- Critics say that it allows too much power to an unnecessary amount of people

The full list of agencies that can now ask for UK citizens' browsing history.

- 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/Army/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
- Common Services Agency for the Scottish Health Service
- Competition and Markets Authority
- Criminal Cases Review Commission
- Department for Communities in Northern Ireland
- Department for the Economy in Northern Ireland
- Department of Justice in 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 Commissioner
- Information Commissioner
- NHS Business Services Authority

- Northern Ireland Ambulance Service Health and Social Care Trust
- Northern Ireland Fire and Rescue Service Board
- Northern Ireland Health and Social Care Regional Business Services Organisation
- Office of Communications
- Office of the 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

jobcentreplus



Threat to Encryption

- Companies now obliged to implement a 'backdoor' into their systems
- The government can request access to the customer's online activity
- These companies can no longer guarantee their user's security and safety.

Jim Killock, the executive director of Open Rights Group, said:

“The UK now has a surveillance law that is more suited to a dictatorship than a democracy. The state has unprecedented powers to monitor and analyse UK citizens’ communications regardless of whether we are suspected of any criminal activity.”

Criticism and Support

- Faced media backlash, but little real resistance.
- Cannot be proven to be a black and white issue - case made to defend from terrorism.
- “If you have nothing to hide, you have nothing to fear.”
- Who is handling your data?

Surveillance

'Extreme surveillance' becomes UK law with barely a whimper

Investigatory Powers Act legalises range of tools for snooping and hacking by the security services

Investigatory Powers Bill: A force for good – if done right?

Bypassing the Act

- VPN/Proxies - routes your data through other networks, making it relatively untraceable.
- Bears resemblance to Great Firewall of China, and internet censorship of Iran and other countries.
- Should the use of proxies be necessary?
- Slow
- Unreliable

The Future

- Officially stated to be a kind of ‘trial period’
- If successful, then will be continued indefinitely.
- Slippery slope of Preventative Surveillance?

Thank you for listening