8.4 Securing liberty online

In the modern digital age, the power of the state and of corporate interests can threaten our privacy and liberty. We have achieved much in rolling back the over-mighty state – passing the first ever Protection of Freedoms Act to restore lost civil liberties, securing the ongoing root and branch review of RIPA and legislating for the creation of a Privacy and Civil Liberties Board – but we cannot be complacent. There will be a complete overhaul of surveillance powers in 2016. We need to ensure this and other opportunities are seized as a chance to control excessive state power, and ensure that in an era when surveillance is easier than ever before, we maintain the right to privacy and free speech. Privacy should always be the norm for personal data, meaning surveillance must always be justified and proportionate and any demand to read private encrypted communications must be targeted and proportionate.

We will:

- Pass a Digital Bill of Rights, to define and enshrine the digital rights of the citizen.
- Safeguard the essential freedom of the internet and back net neutrality, the principle that internet service providers should enable access to all lawful content and applications regardless of the source, and without favouring or blocking particular products or websites.
- Oppose the introduction of the so-called Snooper's Charter. We blocked the draft Communications Data Bill and would do so again. Requiring companies to store a record of everyone's internet activities for a year or to collect third-party communications data for non-business purposes is disproportionate and unacceptable, as is the blanket surveillance of our paper post.
- Set stricter limits on surveillance and consider carefully the outcomes of the reviews we initiated on surveillance legislation by the Royal United Services Institute and the Independent Reviewer of Terrorism Legislation David Anderson QC. We are opposed to the blanket collection of UK residents' personal communications by the police or the intelligence agencies. Access to metadata, live content, or the stored content of personal communications must only take place without consent where there is reasonable suspicion of criminal activity or to prevent threats to life.