LIBERTY
PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Summary of substantive policy discussions at Liberty Council meeting March 2015

UK Government use of "Equipment Interference" more commonly known as hacking

Liberty's Council discussed State hacking. Hacking is an incredibly intrusive surveillance capability that the UK Government has only recently conceded it deploys. In February 2015, the Home Office published a consultation on the UK Intelligence Services use of hacking which revealed that the Government derives authority to hack from broad enabling powers contained in sections 5 & 7 of the Intelligence Services Act 1994. The consultation paper was published on the same day that the Investigatory Powers Tribunal partially upheld Liberty's claim against the Agencies' intelligence sharing relationship with the US.

Council noted that hacking enables the State to conduct the most comprehensive form of surveillance imaginable and has the potential to compromise and destroy the security of individual devices, affected networks, as well as the entire internet. By way of example, computers, laptops, mobile phones, wifi enabled TVs, smart meters etc can all be targeted and once hacked, intelligence agents can access and alter stored data, login details and passwords, browsing histories, emails, diaries, photos, draft documents etc. The weaknesses created can be exploited by anyone else with the required technical knowledge – including criminal hackers. Documents disclosed by former NSA contractor, Edward Snowden, reveal that GCHQ targets network administrators to allow for mass hacking of personal devices.

Liberty's Council discussed the enabling legal framework and the lack of transparency about this practice to date. It agreed a set of bare minimum standards for the use of hacking by the State, including:

1. Primary legislation governing the practice for detailed consideration by Parliament;
2. Authorisation to be granted by way of judicial warrant only in the most serious and narrowly defined set of circumstances, for example with regard to specific threats to life or national security;
3. Hacking should be authorised only in respect of specific individuals or devices suspected of holding evidence;

4. Hacking should not be used to target network administrators or to enable mass surveillance;
5. Warrants should be for a short duration and records of operations securely held;
6. There should be a prohibition on creating, altering or deleting content accessed to preserve the integrity of the criminal justice system;
7. Those whose devices have been hacked should be notified of this once the operation has been concluded unless there are clear grounds for maintaining secrecy.