Liberal Democrats

Safe and Free

Policy Paper 123

Liberty & Security in the UK Policy Paper

Autumn Conference 2016

Contents

Executive Summary

There are unmistakeable threats in the world that can target citizens, even on our own soil – most notably, terrorism. All political parties can agree that we need to protect our citizens. But we disagree about how.

We want a more liberal and effective approach to security policy – an approach that is clear, understandable, community-based, evidence-based, and future-proof.

The threats we face

The government outlined its threats in the 2015 defence and security review. However, there is only one real threat that affects both the liberty and security of UK citizens – terrorism. The threat level in the UK from international terrorism remains consistently high, with international terrorism and groups such as Daesh and Boko Haram causing largescale casualties in their regions.

Counter-extremism and community engagement

A key strand of CONTEST, the counter-terrorism strategy, is Prevent – the community-focused programme that is designed to stop people becoming terrorists or supporting terrorism. The Prevent strategy has many weaknesses – but in our view the key one is that it lacks the trust of the communities it tries to engage. Community engagement is, we believe, the most important aspect of counter-terrorism – it is where information comes from and it is where violent extremism is countered. We would redesign an effective community engagement tool by:

- Scrapping Prevent and replacing it with an inclusive community engagement strategy that would make reporting concerns about extremism the same as reporting concerns about abuse
- Making community engagement an ongoing, core aspect of policing that does not focus solely on counter-terrorism or counter-extremism

- Empowering respected or effective community members who have grassroots credibility to counter the narrative promulgated by violent extremists

Online surveillance

We believe that online surveillance is important to the ability of the police and security services to protect us from threats. We are, however, not convinced that the most appropriate or efficient way of capturing this information is generally via bulk or mass collection of domestic data, as opposed to targeted surveillance of suspects. We are therefore:

- **Opposed** to the indiscriminate bulk collection of Internet Connection Records
- **Opposed** to the indiscriminate bulk collection of communications data (e.g. phone records) by the state
- **Opposed** to bulk Equipment Interference (hacking)
- **Subject to additional safeguards, and in very limited circumstances,** supportive of targeted bulk interception of communications between the UK and certain overseas 'hotspot' areas, where there are no alternative means of safeguarding national security
- **Opposed** to any attempt to systematically undermine encryption

Additional powers of the police and security services

The police and security services also have additional tools available to them, such as offline surveillance and use tools such as detailed police databases. It is our opinion that although the vast majority of these powers are both useful and necessary, they require additional safeguards to ensure that their reach is not unduly extended. We would therefore:

- Require that all police and security services databases be placed on a statutory footing, to ensure that all private information held is subject to oversight and regulation
- Abolish the National Extremist Database, which currently holds detailed accounts of people's movements and political actions even if they have never been arrested.

- Tighten restrictions around Terrorism Prevention and Investigation Measures to ensure that they are used only as a temporary measure in the most serious circumstances where there is a credible threat to life

Regulation of Powers

We believe that authorisation and oversight are key to the operation of the police and security services in a democratic society. It is important not only that regulatory and oversight bodies are independent, but also that they have the powers they need to make their guidance and rulings felt. We would therefore:

- Create a single, independent, public-facing oversight 'Commission' that would help to form a distinction between the approval and post facto audit elements of the oversight body, so Commissioners aren't seen to be 'marking their own homework'
- Strengthen the Investigatory Powers Tribunal, enabling them to award punitive damages to dissuade organisations from breaking the law or their own codes of practice
- In line with the European Court of Human Rights, implement post notification so people are told, where and when appropriate, that they have been under targeted surveillance.

Private information in company hands

Recent years have been characterised by a huge growth in the amount of personal data collected by private companies. This is not a trend that we believe could, or should, be stopped. We do, however, believe that individuals should have control over their own data – and understand the value that is holds. We would therefore:

- Give consumers the ability to access a service even if they do not consent to the sharing of personal data
- Require companies who hold data on identifiable users to contact that person once a year to provide them with a clear and simple explanation of the data held on them
- Require additional consent to be sought from consumers when data is collected for the purpose of the sharing or sale of anonymised data.

Introduction

1.1 Background

1.1.1 Since 9/11, the governments of many countries, including our own, have moved towards large-scale state surveillance systems. This is partly as a result of the rise in the use of personal technology and the opportunities that 'Big Data' presents for intelligence-gathering, and partly because of the increasing threat from terrorism.

1.1.2 Edward Snowden's revelations in 2013 shocked many. That the USA's National Security Agency was tapping the mobile phones of world leaders in allied countries and GCHQ was tapping undersea cables to retrieve data in bulk showed that state surveillance went further than many realised. These revelations led to increased media awareness of the powers afforded to government, the police and the security services.

1.1.3 Domestic and European courts have issued judgments on the collection and retention of data. In 2014 the Court of Justice of the European Union disapplied the European Data Retention Directive which called for member states to record citizens' telecommunications data for up to 24 months, finding it 'constitutes a particularly serious interference with [the fundamental right to privacy and other rights laid down in Article 7 of the Charter]'[1]. The UK courts found the domestic replacement legislation unlawful, though that case has been referred to the European level[2].

1.1.4 The UK and our allies face consistent threats from insurgent and terrorist entities, and with groups and individuals who take their inspiration from them. The police and the security services have been successful in foiling plots to do UK citizens harm time and again and have prosecuted many of

[1] Judgment in C-293/12 (Digital Rights Ireland) http://bit.ly/1XtGpGD
[2] Order of the Court in C-698/15 (David Davis) http://bit.ly/1RNJ1bs

those responsible. The people who work in these fields deserve our grateful thanks, respect and admiration.

1.1.5 These agencies are fighting to protect our citizens' fundamental rights to a private life, freedom of expression, association, conscience and religion that many terrorists seek to deny us. But we must ensure that the powers the agencies have do not undermine the very rights they seek to protect. If the police and security services are seen to be acting reasonably, within a transparent framework consistent with domestic and international law, they will win the trust and confidence of all communities – co-operation that is essential to keep us all safe.

1.2 The current system

1.2.1 We do not have a transparent framework within which the police and the security services currently operate. Existing powers originate from a complex range of different legislation, some of which, due to technological advancement, Parliament never envisaged being used in the way it is now. Most recently, the Investigatory Powers Bill was supposed to bring all surveillance legislation together in one place but it fails to create a single, united approach.

1.2.2 **Online surveillance** is carried out under a number of laws. Currently these include:

- the Data Retention and Investigatory Powers Act 2014 (DRIPA): a time-limited piece of legislation that allows the government to continue to require telephone and internet companies to retain customer records for law enforcement purposes;
- the Regulation of Investigatory Powers Act 2000 (RIPA): Part I allows the collection of communications data (or metadata) and the interception of communications; and

- the Telecommunications Act 1984: Section 94 allows the Home Secretary to give directions of a general character to Communications Service Providers.

1.2.3 These types of surveillance can either be directed at a specific target, or used against, for instance, everyone who lives within a certain area or who uses a certain type of equipment. Such interception of communications is being carried out in ways that are not explicitly allowed in law, although the Investigatory Powers Tribunal has controversially ruled that such interception does not amount to mass surveillance[3].

1.2.4 **Covert and human surveillance** is largely governed by Part 2 of RIPA, which allows the planting of bugs or cameras, and the use of undercover officers and informants. When surveillance involves interference with private property or wireless telegraphy (e.g. bugging someone's home phone) legal authority derives from the Police Act 1997 or the Intelligence Services Act 1994.

1.2.5 **Counter-terrorism activities** are detailed and defined in legislation including the Terrorism Act 2000, the Counter-Terrorism Act 2008, the Terrorism Prevention and Investigation Measures Act 2011 and the Counter-Terrorism and Security Act 2015. Measures introduced in the latter include extending counter-extremism responsibilities to schools and the health service, introducing temporary exclusion from the UK for terrorist suspects, and amending TPIMs.

1.2.6 Counter-terrorism activities are also outlined in the Government's CONTEST strategy. The CONTEST strategy is focused on four areas – Pursue (the investigation and disruption of terrorist attacks, largely using legislation detailed above), Prevent (work to stop people becoming terrorists or

[3] Ruling, IPT - Liberty vs The Security Service & Others http://bit.ly/1RNK1w3

supporting terrorism and extremism), Protect (improving our protective security to stop a terrorist attack), and Prepare (working to minimise the impact of an attack and to recover from it as quickly as possible).[4] The most well-known of these areas is the Prevent programme, which includes Channel - the community-focused 'de-radicalisation' programme.

1.2.7 **Counter-extremism** is currently managed through the Government's CONTEST strategy, with plans to bring forward a Counter-Extremism and Safeguarding Bill in the 2016/17 parliamentary session. The strategy defines extremism as: *'the vocal or active opposition to our fundamental values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faiths and beliefs. We also regard calls for the death of members of our armed forces as extremist.'* To combat extremism, it calls for the countering of extremist ideology, the building of a partnership with all those opposed to extremism, the disruption of extremists and the building of more cohesive communities.

1.2.8 **Immigration and nationality powers** allow the Government to ban extremists from entering the UK and remove the passports of those suspected of terrorist activities while abroad, even if that renders those people stateless.

1.3 A Liberal Approach

1.3.1 Liberal Democrats regard some of the powers that the state has acquired or is looking to acquire as over-broad, poorly understood and illiberal. More than that, they have the potential to be ineffective and counterproductive. As part of the Coalition Government, we worked to improve some of the most egregious examples of state overreach – abolishing ID cards for example.

[4] CONTEST Annual Report for 2014 (latest available) http://bit.ly/1WuhqEg

1.3.2 The Snowden revelations, the growing concerns over the use of Prevent, the current Investigatory Powers Bill and the upcoming Counter-Extremism and Safeguarding Bill, all show that we need to have a clear liberal policy on these issues. The whole country suffers when teachers feel that they cannot encourage an open discussion of British foreign policy in the classroom, when communities feel they are subjected to disproportionate and unfair scrutiny, and when individuals feel targeted because of their faith or their ethnic background. Our united stance against terrorism is undermined.

1.3.3 We advocate a liberal and effective approach to security policy that is understandable to citizens; clearer for the police and the security services, which is more community-based, evidence-based and future-proof. We endorse and adopt the Ten Tests for the Intrusion of Privacy included in RUSI's Report of the Independent Surveillance Review[5]:

1) **Rule of law**: All intrusion into privacy must be in accordance with law through processes that can be meaningfully assessed against clear and open legislation, and only for purposes laid down by law.
2) **Necessity**: All intrusion must be justified as necessary in relation to explicit tasks and missions assigned to government agencies in accordance with their duly democratic processes, and there should be no other practicable means of achieving the objective.
3) **Proportionality**: Intrusion must be judged as proportionate to the advantages gained, not just in cost or resource terms but also through a judgement that the degree of intrusion is matched by the seriousness of the harm to be prevented.
4) **Restraint**: It should not be routine for the state to intrude into the lives of its citizens. It must be reluctant to do so,

[5] 'A Democratic Licence to Operate', RUSI 2015 http://bit.ly/1RNMgzq

restrained in the powers it chooses to use, and properly authorised when it deems it necessary to intrude.

5) **Effective oversight**: An effective regime must be in place. Effectiveness should be judged by the capabilities of the regime to supervise and investigate governmental intrusion, the power it has to bring officials to account, and the transparency it embodies so the public can be confident it is working properly. There should also be means independently to investigate complaints.

6) **Recognition of necessary secrecy:** The 'secret parts of the state' must be acknowledged as necessary to the functioning and protection of the open society. It cannot be more than minimally transparent, but it must be fully democratically accountable.

7) **Minimal secrecy:** The 'secret parts of the state' must draw and observe clear boundaries between that which must remain secret (such as intelligence sources or the identity of their employees) and all other aspects of their work which should be openly acknowledged. Necessary secrecy, however, must not be a justification for a wider culture of secrecy on security and intelligence matters.

8) **Transparency:** How the law applies to the citizen must be evident if the rule of law is to be upheld. Anything that does not need to be secret should be transparent to the public; not just comprehensible to dedicated specialists but clearly stated in ways that any interested citizen understands.

9) **Legislative clarity**: Relevant legislation is not likely to be simple but it must be clearly explained in Codes of Practice that have Parliamentary approval, are kept up-to-date and are accessible to citizens, the private sector, foreign governments and practitioners alike.

10) **Multilateral collaboration:** Government policy on intrusion should be capable of being harmonised with that of like-minded open and democratic governments.

The threats we face

2.1 National Security Strategy

2.1.1 In November 2015, the government published the *National Security Strategy and Strategic Defence and Security Review 2015*. It detailed our security objectives and the changing threats we face. Four broad challenges to the UK's security priorities are listed in the strategy, followed by a number of specific concerns.[6] Only two are relevant to the 'Liberty and Security' remit of this paper and our focus will therefore primarily be on the threats posed by terrorism and extremism. The review details these threats thus:

2.1.2 **The increasing threat posed by terrorism, extremism and instability.** Terrorism and extremism, including the threat to British nationals overseas, where 60 British nationals have been killed since 2010. The complexity of terrorist plots varies from knife and gun attacks to firearms and explosives at multiple locations. Extremist groups have exploited the internet to distribute propaganda intended to radicalise and recruit from the UK and elsewhere. Extremism is only mentioned as a threat in reference to violent extremism and terrorism. State collapse and state-wide terrorism also has an effect on instability, which has contributed to the refugee crisis from Syria and the Middle East, compounded by long-term issues in countries such as Afghanistan, and also widespread displacement within Africa. There remains a threat from violent dissidents in Northern Ireland.

2.1.3 **The impact of technology, especially cyber threats; and wider technological developments.** Cyber threats from states and non-state actors, such as terrorists and hackers are detailed, including the difficulty of keeping data collected from other states and the private sector secure. Medical

[6] National Security Strategy and Strategic Defence and Security Review, November 2015 http://bit.ly/23URLDm

technology, issues of Western states' technological advantage, access to space and near-Earth orbits, as well as innovative defence and security industries are also referenced.

2.2 Terrorism

Threat Levels

2.2.1 The 'National Threat Level' is an independent, publicised measure of the current threat from terrorism. It is the clearest measure of anticipated threats to the nation that do not originate in the traditional area of open interstate warfare. Threat levels are decided based on available intelligence, terrorist capability, terrorist intentions and timescale.

2.2.2 There are three published threat areas: (1) the threat to the UK from international terrorism, (2) the threat of Northern Ireland-related terrorism in Northern Ireland and (3) the threat of Northern Ireland-related terrorism in Britain. There are five possible levels: Low (an attack in unlikely), Moderate (an attack is possible, but not likely), Substantial (an attack is a strong possibility), Severe (an attack is highly likely) and Critical (an attack is expected imminently). Since 2006, the threat level for international terrorism in the UK has never been below 'Substantial'. The Northern Ireland measurements have been published since 2010. The threat in Northern Ireland from separatist violence has never been below 'Severe'.

2.2.3 The threat levels in May 2016 were:

- SEVERE for international terrorism in the UK.
- SEVERE for Northern Ireland-related terrorism in Northern Ireland.
- SUBSTANTIAL for Northern Ireland-related terrorism in Britain.

The threat of terrorism

2.2.4 Terrorism remains a global problem. The Global Terrorism Index for 2015 reported that terrorist activity had increased by 80% in 2014 to its highest recorded level. There were 32,685 deaths from terrorism in 2014, a nine-fold increase since the year 2000. Terrorist activity remains highly concentrated with Iraq, Nigeria, Afghanistan, Pakistan, and Syria, which collectively account for 78% of deaths. International focus is on Daesh, but in 2014 Boko Haram accounted for 6644 deaths and was the terrorist group responsible for most deaths in 2014. In addition, there were 19 wars recorded by the Heidelberg Institute in 2015, many of which had a terrorist element, including in Pakistan, Nigeria, and Turkey.

2.2.5 In Europe, in addition to threats over the last few decades from Northern Irish terrorism, militant animal rights activists, and the far right, there is also a growing trend of far right violent extremism – self-identified fascist Anders Breivik is the most notable example.

2.2.6 Attacks in Paris and Brussels over the last year have resulted in the deaths of 162 people. The attacks in France were the deadliest in the European Union since the Madrid train bombings of 2004. While these have understandably raised concerns about attacks in the UK, they have not affected the UK threat level which has remained at SEVERE since October 2012. This can partly be seen as a result of the pre-existing high threat level and partly of the circumstances in the UK that present further challenges to potential attackers, for example gun control and border control where all passports are checked against watch lists.

2.2.7 Recent attacks have had a distinctive character. They have focused on crowded, public spaces, and have involved co-ordinated multiple active shooters and bombs. British police and security services have been preparing for this scenario since similar attacks in 2008 in Mumbai.

2.2.8 After the Brussels attacks, the Home Secretary Theresa May told Parliament that the police and security services had disrupted seven terrorist plots to attack the UK in the 18 months to March 2016. All those plots were either linked to, or inspired by, Daesh and its propaganda. The October 2015 Counter-Extremism Strategy stated that 40 terrorist plots have been disrupted since the London bombings in 2005 with the 'overwhelming majority' inspired by Islamist extremists.

Policing terror

2.2.9 There were 299 terrorist-related arrests in the year to March 2015, an increase of 31% from the previous year. Of these, 100 people had (as of March 2016) been charged with a terrorism-related offence and 18 with other offences; 130 had been released without charge. Three out of four (76%) of those arrested identified their nationality as British. Since 2001, only 16% of those arrested for a terrorism-related offence have been convicted. 52% have been released without charge. Over the same time period, arrests resulting from stop and search powers under the Terrorism Act 2000 have never exceeded 7%.[7]

Concerns about terrorism

2.2.10 A January 2016 YouGov poll of global issues in 17 countries found showed 26.1% of British people were concerned about global terrorism, about average.[8] The YouGov June 2015 poll showed an increase, from 9% to 14%, in the number of people believing there was a 'high' chance that they, a member of their family, or a good friend would be killed or wounded in a terrorist attack, despite the official threat level remaining the same. Over half of the people

[7] Main Tables: Terrorism Statistics (Year to 31 March 2015), Home Office http://bit.ly/1TVmL3A

[8] 'Global survey', YouGov press release 29/01/2016 http://bit.ly/24UsHyV

surveyed (55%) believed the chances were 'low' and 19% believed the chances were 'almost non-existent'.[9]

2.2.11 Although the threat from terrorism remains high, David Anderson QC, the Independent Reviewer of Terrorism Legislation said in his 2013 report:

> *'During the 21st century, terrorism has been an insignificant cause of mortality in the United Kingdom. The annualised average of five deaths caused by terrorism in England and Wales over this period compares with total accidental deaths in 2010 of 17,201.'* [10]

Hate Crimes

2.2.12 Concerns about terrorism that lead to violence or, more widely, hostility amongst some individuals and groups towards people from different ethnic or religious backgrounds have been increasingly prevalent in recent years. Islamophobia is increasing, as are anti-Semitic attacks and attacks based on homophobia and transphobia. After Islamist terror attacks in Paris, for instance, attacks on Muslims in London tripled. These attacks are hate crimes – they are inexcusable, entirely unjustified, and should result in the prosecution of those involved.

2.3 Extremism

2.3.1 The Government's Counter-Extremism Strategy asserts that '[British] values are under attack from extremists operating at a pace and scale not before seen'. The strategy raises concerns regarding the promotion of hatred and hate crime, the encouragement of personal and societal isolation, certain forms of religious law, a rejection of the democratic system, harmful and illegal cultural practices such as FGM and forced marriage, and institutional failure to combat extremism in

[9] 'Terrorism concerns highest since 7/7', YouGov press release 30/06/2015 http://bit.ly/24Uss6N

[10] The Terrorism Acts in 2011, David Anderson QC http://bit.ly/24UpuPH

schools, universities, local authorities, charities, and prisons. To deal with the broad challenge of extremism, the Government has four areas of focus.

2.3.2 **Countering extremist ideology.** The Government asserts that extreme ideologies are used to radicalise and recruit vulnerable audiences to violent extremism over social media and online mediums. The Government aims to implement a counter-ideology campaign by contesting the online space, strengthening institutions, and supporting individuals at particular risk of radicalisation.

2.3.3 **Building a partnership with all those opposed to extremism.** The Government says it will develop a new network of individuals and groups who have credibility and experience fighting extremism within their communities. They intend to continue to avoid engaging with extremists by not meeting or working with them.

2.3.4 **Disrupting extremists.** This focuses on targeting extremists with legislation and includes reviewing rules on citizenship, banning extremist organisations, restricting the harmful activities of the most dangerous extremist individuals and restricting access to premises which are repeatedly used to support extremism.

2.3.5 **Building more cohesive communities.** The Government proposes to build on existing programmes such as the National Citizen Service, English language classes, and initiatives to tackle FGM / violence against women and girls. The Government will put together a Cohesive Communities Programme to focus on local interventions.

2.4 Cross-border crime

2.4.1 Cross-border crime is a growing problem including the trafficking of drugs, firearms and people for exploitation – criminals do not respect boundaries, whether police force boundaries or national ones. This is especially the case with cybercrime, where the decentralised nature of the internet means that this type of crime is almost inherently cross-border. The first England and Wales crime figures to include cybercrime estimated 5.1m online fraud incidents and 2.5m cybercrime incidents in the 12 months to June 2015.

Britain in Europe

2.4.2 Membership of the EU enhances UK security. Measures such as the European Arrest Warrant speeds up the extradition process and ensures offenders are returned to the UK to stand trial. Since 2010 916 suspects have been returned to the UK to face trial under the EAW and 9,305 have been extradited from the UK to other European countries.

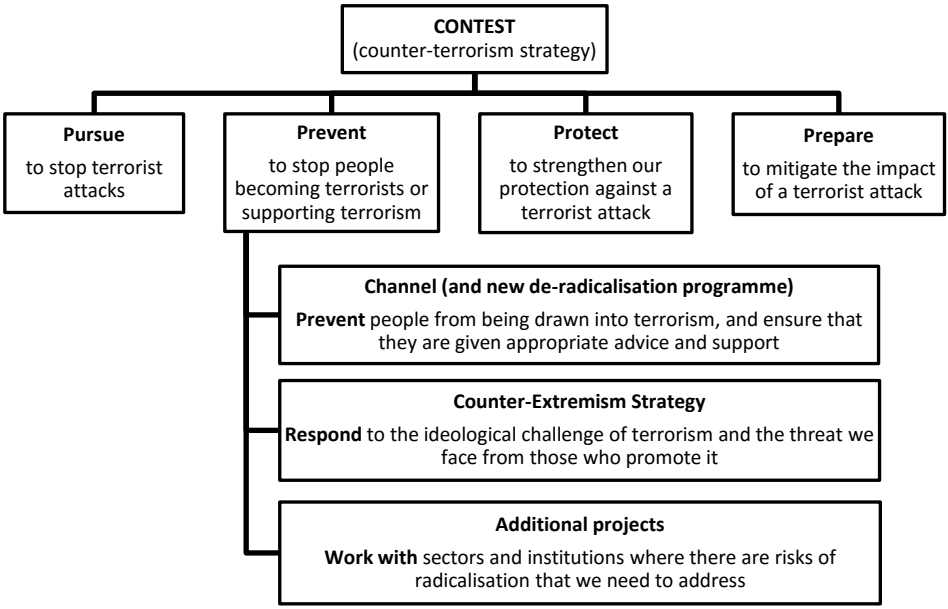
2.4.3 The UK also participates in the Prüm decision, which allows rapid matching of DNA profiles, fingerprints and vehicle registration marks across member states – a process that would otherwise take months. Personal information is only provided once certain scientific thresholds have been reached and only if the offence is sufficiently serious.

2.5 Responding to threats

2.5.1 The key threat to national security within the United Kingdom is terrorism. The response of the UK government has been primarily increased surveillance, expanding counter-terrorism policing and the intelligence services, and overseas interventions. Liberal Democrats do not believe a surveillance strategy alone to be either effective or sustainable without further supporting measures.

2.5.2 Liberal Democrats believe that more emphasis should be placed on community engagement and addressing the root causes of terrorism. Bolstering community policing and supporting and empowering communities will increase trust and confidence, enhance the flow of community intelligence, and reduce the factors that give rise to disaffection and radicalisation. This renewed approach to community engagement and counter-extremism will mitigate the need for some of the more controversial counter-terrorism legislation.

Counter-Extremism and Community Engagement



3.1 The current system

3.1.1 In the current system Pursue, Protect, and Prepare concentrate on the work of the security services, addressing vulnerabilities, and building resilience respectively. Prevent is the tool that focuses on the community engagement and 'de-radicalisation' aspects of counter-terrorism. It is supposed to avert threats by stopping people participating in terrorism.

3.1.2 Within the Prevent Strategy, Channel is the most controversial strand. Channel is coordinated by the police and designed to act as a form of early de-radicalisation for people about whom concerns have been raised.

- In 2013/14, there were 1,281 Channel referrals. **From Jan-Aug 2015 there were 2,811 referrals.**
- By the end of 2013/14, only o**ne in five of these referrals resulted in action being taken.** It has also not been made clear what specific behaviours required further action to be taken.
- Between 2012 and March 2014, **Muslims accounted for 84% of referrals where religion was known.**
- **Nearly 40% of referrals were under the age of 18.**

3.2 The Extremist 'Conveyor Belt'

3.2.1 The Prevent Strategy is based on the simplistic claim that non-violent extreme ideologies necessarily lead to some adherents becoming terrorists (the so-called 'conveyor belt' theory). Indeed, one of the guiding principles of the Prevent Strategy, published in 2011 states: 'We remain absolutely committed to protecting freedom of speech in this country. But preventing terrorism will mean challenging extremist (and non-violent) ideas that are also part of a terrorist ideology.'

3.2.2 The 'conveyor belt' theory is contested by academics[11] and counter-terrorism experts – even the Government has not presented a united front. Leaked papers to the Cabinet's Home Affairs committee from 2011 reveal disunity: 'It is sometimes argued that violent extremists have progressed to terrorism by way of a passing commitment to non-violent Islamist extremism… We do not believe that it is accurate to regard radicalisation in this country as a linear 'conveyor belt' moving from grievance, through radicalisation, to violence … This thesis seems to both misread the radicalisation process and to give undue weight to ideological factors.'[12]

3.2.3 The theory is also undermined by the profile of terrorists involved in recent attacks who were already known to police

[11] E.g. *A Decade Lost* by Prof Arun Kundnani, 2015 http://bit.ly/1RN4m4H
[12] 'Hizb ut Tahrir is not a gateway to terrorism', Sunday Telegraph 25/07/2010 http://bit.ly/1WBRztC

for crimes unrelated to terrorism. The perpetrators of the Brussels attacks, for instance, were known to the police for their involvement in organised crime. Two of the Paris attackers had been jailed in 2010 for armed robbery. Meanwhile, the Provisional IRA (formally disbanded) has moved into vigilantism with a group called 'Direct Action Against Drugs', where former paramilitaries have run a long campaign of assassination against Belfast drug dealers, culminating in 2015 with in a number of murders of former PIRA members. In these scenarios, it is not religious or political extremism that turns into violence, but pre-existing criminality and/or a failure to submit to the rule of law.

3.2.4 We remain unconvinced that non-violent extremism necessarily or regularly leads directly to a threat to public safety. There are, undoubtedly, many other risk factors that are involved, and which may not be subject to such stringent action under Prevent, including vulnerability, alienation, criminal involvement, and active recruitment. Additionally, the role of political (rather than religious) radicalisation in recruitment particularly to groups such as Daesh should not be underestimated.

3.2.5 The 'conveyor belt' theory also ignores many of the wider factors involved in violent extremism and does not adequately explain the many people who hold what we may consider to be extreme views, but who do not tend towards violence in any way. There are sizeable fundamentalist Christian and ultra-orthodox Jewish groups both in the UK and overseas populations who are not believed to pose any realistic threat whatsoever. From a Liberal Democrat perspective, the issue of social integration and divided communities is a concern, but not a subject for this working group – and it is our recommendation that it should be examined in detail by another group during this Parliament.

3.3 Problems with the Prevent Strategy

3.3.1 **A lack of trust in Prevent** amongst the communities it attempts to rely on to provide community intelligence. David Anderson QC, Independent Reviewer of Terrorism Legislation, said in his submission to the Home Affairs Selection Committee's inquiry into countering extremism "the lack of confidence in aspects of the Prevent programme, particularly but not exclusively among Muslims, is undeniable…[it] is clearly suffering from a widespread problem of perception"[13]. The problem of perception is a very real one when it comes to community engagement, as it undermines trust and confidence in the police and security services. The perception that Prevent is focused on British Muslims has not been helped by statements from the Northern Ireland Office that Prevent will not be extended to Northern Ireland[14]. The approach of Prevent is so discredited amongst those communities where success is important that an entirely new approach is needed – doing nothing or a simple rebranding will not do.

3.3.2 **The focus on non-violent extremism.** Tied to the 'conveyor belt' theory, there is a sense that Prevent is focused on stamping out non-violent extremism or to put it another way, clamping down on free lawful speech, appearance or conduct that the Government does not like. As detailed above, the evidence that non-violent extremism leads to terrorism is lacking. There are undoubtedly other factors associated with people being drawn into violent extremism that need to be addressed including: the absence of a sense of belonging, a sense of hopelessness or that ambitions cannot be achieved through conventional routes, a sense of not being listened to or not being unable to influence issues

[13] David Anderson QC, submission to the Home Affairs Select Committee 29/01/2016 http://bit.ly/1TFXebN
[14] Counter-terrorism: Northern Ireland, written question 5119 01/07/2015 http://bit.ly/1TFZtfr

that people are passionate about; and a general sense of being alienated by government and/or society.

3.3.3 **Prevent and Channel are opaque and lacking in oversight.** The 2014 Annual Report for Prevent states 'We have a network of dedicated Prevent co-ordinators in 30 priority Local Authority areas and are supporting important projects in a further 14 areas. More than 180 local projects have been delivered, including education, internet safety, and work with families, reaching over 55,000 people since early 2012.' This, however, is the only information publicly available. Despite repeated questions in Parliament, the Home Office will not provide a breakdown of project spending, nor details of how local authority spending is allocated. There are also no published evaluations and no publicly available indicators of success, making it impossible to independently judge the impact and outcomes of Prevent. It is entirely possible that some interventions are counter-productive, helping to create rather than diminish the problems they seek to address. This is also true of Channel, where there is no clarity as to what criteria are used to warrant further action, and no understanding of what 'further action' means for individuals. Anecdotally, we understand that recruitment and retention of Prevent co-ordinators in the 30 priority Local Authorities is proving difficult.

3.3.4 **Impact on free expression in education.** Since 2015, teachers have been placed under a statutory duty to report extremism – a responsibility that Trade Unions such as the NUT have contested. The University and College Union have also expressed their opposition to Prevent as far as universities are concerned. The Government aims to portray this responsibility as an extension of safeguarding, which is already in place, for example, for FGM. On a recent visit to the UK the UN's special rapporteur on the right to freedom of assembly stated: "The spectre of Big Brother is so large, in fact, that I was informed that some families are afraid of discussing the negative effects of terrorism in their own

homes, fearing their children would talk about it at school and have their intentions misconstrued." Similar concerns have also been expressed in other sectors too, given the wide-reaching nature of 'Prevent' - in health, charities and financial services, to name but a few.

3.3.5 The Counter-Extremism Strategy provides support or encouragement to policies that go beyond protesting at someone's views or attendance at an event, or go beyond simply choosing not to invite someone to speak. Instead they aim to deny lawful freedom of expression to individuals, with views considered to be controversial or offensive, after they have been invited to speak. **We do not believe that this prior restraint of speech is something the Government should encourage nor that public bodies (especially Universities) should allow.**

3.3.6 Refusing to permit the free expression of lawful views with which one disagrees is counter-productive and risks creating free speech martyrs. It does not help to build a counter-narrative, does not help to undermine extreme views by challenging them, risks driving contentious speech "underground" with fewer safeguards, and undermines rights to free expression. Nor do we believe that it is either workable or liberal to allow public sector educational bodies to insist that groups or individuals organising speaker events should be required to have an 'opinion-balanced panel' of speakers ("forced platform"). This would require knowledge of what was to be said and seriously curtail the rights of free association of campaign groups and communities.

3.3.7 It would be better, and far more practical, where University (or other) authorities have reasonable grounds to fear that speech may over-step the grounds of lawfulness, for the University to insist (as a condition of the meeting taking place) on the proceedings being recorded so that complaints about illegal speech can be evidenced afterwards.

3.3.8 **Vague and generalised indicators.** Examples of indicators of potential involvement with terrorism or extremism are wide-ranging and by no means particular to people involved in terrorist-related activity. For instance, in Channel's Vulnerability Assessment Framework, indicators include 'feelings of grievance and injustice', 'a desire for political or moral change', 'being at a transitional time of life', 'over-identification with a group or ideology' and 'individual knowledge, skills and competencies'. By comparison, indicators of joining a gang are much more targeted, including 'unexplained money or possessions', 'committing crimes such as shoplifting', or 'physical injuries'. As well as causing undue worry to parents and guardians, these generalised indicators provide little help for those with concerns. It is not surprising that there are large numbers of referrals to Channel where no further action is taken.

3.4 What community engagement should look like

3.4.1 **Liberal Democrats would scrap Prevent in its entirety.** Prevent and Channel are discredited amongst those communities where their success is most important. The importance of cultivating community relations in preventing the development of terrorism cannot be overstated, but Prevent can no longer be the vehicle by which this is delivered.

3.4.2 Prevent should be replaced with a community-focused strategy with a more positive name such '**Engage'.** It would:

- **Mainstream reporting procedures for all aspects of wellbeing.** Concerns about extremism would be communicated in the same way as concerns about involvement with gangs, child abuse, or grooming, so as. This aims to avoid the current Islamophobic focus. We recommend making use of existing local safeguarding boards – for both children and adults.

- **Remove absolute control from the Home Office,** sharing with the Department for Communities and Local Government control over aspects of the strategy such as promoting counter-narratives and promoting integration of minority communities.
- **Decentralise and disclose funding and measurements of success,** with Principal Local Authorities making support decisions based on their local areas.
- **Openly debate extremists and promote a real counter-narrative** by working with mainstream community voices that have grassroots credibility.
- **Amend the use of 'British values' to 'universal democratic values'** – the way that the Conservative government has been using 'British values' is divisive, rather than inclusive – we would refer to 'universal values' instead, whilst continuing to defend the gains we have made in liberalism and equality.
- Take every opportunity to **reinforce that different communities are integral to a liberal democracy.**
- **Publish clear, easy to understand information and statistics** that allow independent scrutiny of the strategy and increase transparency of outcomes.
- **Promote the integration of minority communities** wherever they exist, including by enhancing outreach work and English language teaching for adults.

3.4.3 Engagement should **empower respected or effective community members who have grassroots credibility** to counter the narrative promulgated by violent extremists. This would not be a facet of a wider project, but the primary focus of it. It will require that these individuals and groups have the funding and technical support necessary to challenge violent extremism without undermining their independence or credibility. The Department for Communities and Local Government should provide comprehensive advice and support on how best to engage with communities when developing a pluralistic, credible counter-narrative.

3.4.4 Community engagement **should not focus solely on counter-terrorism or counter-extremism.** This leads to mutual suspicion, ineffective communication and the overlooking of the other risk factors that are not ideologically based.

3.4.5 **Community engagement should be an ongoing, core aspect of policing.** This was a lesson learned in Northern Ireland after the Good Friday Agreement, and one that the 2001 Cantle Report in mainland Britain, which took a wide view of community cohesion and the role of the police and public services, also developed[15]. We agree with the Patten report into Northern Ireland's policing that 'the term 'Community Affairs' suggests us… that working with the community is seen as a specialist activity… a good thing to do if you can spare the officers and the time to do it, but not the main function of the police…. We believe that neighbourhood policing should be at the core of police work.'[16]

3.4.6 **Police and security service powers must be necessary, proportionate and implemented without discrimination.** This will help justify the powers to the community. This applies to all aspects of law – but is particularly relevant when it comes to terrorism and extremism legislation given the communities that it affects most.

3.4.7 **Recognition of the impact of foreign affairs policy and activity** on communities. It is important for the Government to engage with and explain to domestic communities who have links to affected areas, why foreign intervention is supported by the UK – especially where this includes the involvement of British Armed Forces. We should also encourage the democratic participation of people who seek a different

[15] Community Cohesion: A Report of the Independent Review Team, 2001 http://bit.ly/1VM8vgj
[16] A New Beginning: Policing in Northern Ireland, 1999 http://bit.ly/1qqJFFF

approach. As David Anderson said in 2013, "foreign military interventions can be cynically exploited by agents of radicalisation. They cannot, of course, excuse acts of terrorism. It is idle however to pretend that foreign policy has not been an influence in radicalisation".

3.4.8 **Promote debate and counter-narratives** rather than refusing to engage with, or simply criminalising, those that we disagree with. We believe that the Government's policy of refusing to engage with people or organisations it believes to be 'extremist' is neither effective nor productive. It leaves members of the law-abiding public without a democratic voice at governmental level. The Conservative Government's failure to engage with groups such as the Muslim Council of Britain has a direct impact upon their ability to gather opinion and test or exchange policy ideas.

3.4.9 The **Privacy and Civil Liberties Board legislated for in the Counter-Terrorism and Security Act 2015 and abandoned by the Conservatives in government should be immediately established.** The Board should engage in the task of reviewing the operation of terrorism legislation, particularly with a view to the impact of these laws on those sections of society that they are most used against.

3.4.10 **Take action to address educational underachievement and lack of employment prospects** amongst those minority communities and socio-economic groups affected. Discrimination in the jobs market, the workplace and the criminal justice system, low family income, below standard schooling and lack of job opportunities in some areas, have a detrimental effect on the life chances of some groups. Addressing these issues can help to reduce disillusionment and underachievement that can provide a push people towards violent extremism.

3.4.11 **Address grooming and radicalisation more comprehensively in high risk situations, including working**

towards solving underlying issues that contribute to the risk. This is particularly the case in prisons, where there have been reports that 'Islamic radicalisation' has become a problem. We believe that the Government's tendency to conflate religious extremism and terrorism fuels the issue of radicalisation – especially in prison, a clear line needs to be drawn between extremism and violent extremism. It is clear, though, that prison populations are a particularly at risk group who are more likely to be socially isolated, have few educational qualifications, lack sufficient employment opportunities on release, and are in an exceptional situation where physical coercion can be prevalent. Thus, prisoners need careful and specialised support to reduce the risks of grooming or radicalisation. Liberal Democrats would also reduce prison overcrowding by encouraging the use of community sentences and diverting non-problematic drug users away from the criminal justice system.

3.4.12 **Extend the new 'Engage' strategy to Northern Ireland,** so demonstrating that all forms of violent extremism are being seriously tackled.

Online Surveillance

4.1 Background and Summary

4.1.1 Outside counter-extremism, the police and security services need to ensure that citizens remain safe from threats – from violent extremism and terrorism, from cyber-attacks, from hostile foreign powers and from serious and organised crime. One way of identifying and monitoring these threats is some form of online surveillance.

4.1.2 It has been variously argued that the UK does not engage in mass surveillance, that 'the indiscriminate trawling for information by interception, whether mass or bulk or otherwise, would be unlawful', and that surveillance is not indiscriminate but rather 'discriminate (in the sense that it is within very broad selectors) but vast'. In the most general sense, **it is our opinion that targeted, more intrusive surveillance is preferable to bulk or mass collection of data.**

4.1.3 Some commentators argue that the collection of personal data does not interfere with privacy rights. Others suggest that data can even be filtered and analysed by automated systems, and that privacy is still intact as long as no human eye has looked at the material. **We reject these arguments.** We agree with David Anderson who says 'in the context of investigatory powers, [Article 8 – the right to a private life] is engaged not only when material is read, analysed and later shared with other authorities, but also when it is collected, stored and filtered, even without human intervention.'

4.1.4 Privacy is not an unqualified right under Article 8 of the European Convention of Human Rights, but interference with it has to be necessary and proportionate. For breach of Article 8 to be lawful, it normally requires that such interference is targeted and done on the basis of reasonable

suspicion. When the data in question is collected in bulk on large numbers of people who have done nothing criminal, breach of Article 8 becomes difficult to justify.

4.1.5 As this chapter will describe, Liberal Democrats:

- Are **opposed** to the indiscriminate bulk collection of Internet Connection Records
- Are **opposed** to the indiscriminate bulk collection of communications data (e.g. phone records) by the state
- Are **opposed** to bulk Equipment Interference (hacking)
- **Subject to additional safeguards, and in very limited circumstances,** support targeted bulk interception of communications between the UK and certain overseas 'hotspot' areas, where there are no alternative means of safeguarding national security
- Are **opposed** to any attempt to systematically undermine encryption

4.2 What is bulk data and who collects it?

4.2.1 'Bulk' data collection refers to the collection by the state of undifferentiated data relating to multiple individuals and devices, usually by collecting data in aggregate from internet-connected services. In short, it is the collection of information about the online activity of large numbers of people, the vast majority of whom are not under investigation. Once collected, it is analysed in order to find out more about known suspects and their associates, and to develop new leads. 'Bulk' can be an unhelpful term, as bulk collection may include a degree of targeting. It can refer to the collection of massive amounts of data at the population level; but it can also refer to much smaller operations focused on a particular area or network.

4.2.2 Bulk collection is carried out by different UK agencies. The most significant is GCHQ, which uses its powers under section 8(4) of RIPA to tap internet cables in order to collect, store and analyse the content and metadata of communications where one end is located overseas. GCHQ does not seek to collect

communications where both ends are in the UK, in bulk, although this can happen inadvertently.

4.2.3 MI5 collects bulk metadata (who called whom, where they were and when) relating to all telephone calls made inside the UK, under powers in the Telecommunications Act 1984. The existence of this power was secret until the Home Secretary avowed it when the draft IP Bill was published in 2015. **We oppose this collection.**

4.2.4 Communications Service Providers (CSPs, usually internet providers and telephone companies) retain bulk data (predominantly phone records and subscriber details) on their customers for a maximum of 12 months. This data would already be retained by CSPs for business purposes, if for a shorter amount of time. This has been a long-standing arrangement under DRIPA and before that by the EU Data Retention Directive. **We accept that the collection of this business data by CSPs is necessary for law enforcement purposes, subject to appropriate UK and EU law.** We do not agree with CSPs being required to create and collect bulk new datasets which they do not need for their own business purposes. We would also ensure that service providers are not mandated by law to collect in bulk third-party communications data for non-business purposes by any method.

4.2.5 The Investigatory Powers Bill will replace all of these powers, which will remain in force under the new statute. The Bill will also significantly extend the scope of bulk collection and retention by CSPs by requiring them to collect and store 'Internet Connection Records' – records of apps, services and websites accessed. 'Internet Connection Records' is a misnomer – they are the retention of UK citizens' web history. It is the pre-internet equivalent of hiring a private investigator to follow every person in the UK and record their movements, on the grounds that it may be useful at some point in the next year.

4.2.6 We believe the blanket retrospective collection of the Internet Connection Records (ICRs) of the entire British population is unnecessary and disproportionate. These records are capable of revealing many aspects of our daily lives in great detail. Liberal Democrats who served as ministers in government in 2012-13 when similar proposals were put forward are clear that no compelling operational case was advanced. That situation has not changed. Not only has the case not been made for ICRs, but the experience in Denmark (where ICRs were introduced and later repealed) suggests that they have limited utility and risk swamping the police with irrelevant data.

4.2.7 We agree that it would desirable for law enforcement to be able to access records that shows which temporary IP address a device was assigned at a particular point in time. There is a particular problem in child sexual exploitation investigations where servers have been seized which contain the logs of IP addresses that accessed images of child abuse, but those records cannot be traced back to individual devices due to the fact that IP addresses are shared widely between devices and no records are kept of these matches. We passed legislation in 2015 to allow for the retention of dynamic IP matching data, but the powers appear to have been poorly drafted by the Home Office and have proved ineffective in practice. While the police should be able to establish which devices accessed illegal websites, we believe this could and should be done without storing everyone in the UK's web history for 12 months. **We believe that much more work needs to go into designing a system that allows IP matches to be logged without collecting the far more sensitive ICRs proposed under the Investigatory Powers Bill.**

4.2.8 While we are firmly opposed to the indiscriminate collection of ICRs, we accept that there are circumstances in which ICRs can be a useful tool for investigating known suspects. For

that reason, we would allow the police under the authority of judicial commissioner warrant to require CSPs to retain the web histories of individuals once reasonable suspicion has been established.

4.2.9 We welcome the Home Secretary's decision to ask the Independent Reviewer of Terrorism Legislation to review the efficacy of bulk powers. But we caution against the possibility of drawing a permanent conclusion from a review of current capabilities. If the review concludes that any bulk powers are both necessary and proportionate, the constant development of technology and/or the changing nature of security threats mean that they may not remain so. **Any legislation allowing for bulk powers should contain a clause for a future reviews at regular interviews.**

4.3 Constraints

4.3.1 Article 8 of the European Convention on Human Rights requires that any access to personal data by law enforcement or the intelligence agencies must be 'necessary and proportionate'. This means that indiscriminate trawling of bulk data is not allowed and queries have to be in connection with specific investigations. Agency staff that are accessing the data are audited and have to be able to account for their actions. Where bulk data reveals a suspect who is located in the UK and the authorities want to access the content of their communications, a warrant must be sought from the Home Secretary.

4.3.2 While the concepts of necessity and proportionality are very useful, they are also highly subjective. The Snowden revelations highlighted a number of operations which have been criticised as disproportionate by privacy advocates, either because of collateral intrusion into the private lives of innocent people (disproportionate), or because they involve covert intrusion into the network infrastructure of companies based in

Europe, where formal intelligence sharing arrangements could have been used instead (unnecessary).

4.4 Opinions on bulk data collection

4.4.1 Liberal Democrats believe that the collection of personal data on innocent people by or at the request of the state interferes with our right to privacy, regardless of whether that data is ultimately seen by an investigator.

4.4.2 Privacy is not an absolute right: there are circumstances in which the public interest in preventing crime outweighs the rights of the individual suspect. But the infringement of privacy must be justified in every case and we are therefore instinctively opposed to the use of dragnet techniques which trawl the data of millions of innocent people, in order to identify a small number of criminals.

4.4.3 The key question is how we can ensure that legitimate surveillance systems are designed in such a way that they avoid collecting innocent persons' data.

4.4.4 It is argued that espionage conducted against non-UK citizens requires less justification than surveillance conducted on our own citizens. **Liberal Democrats do not accept the premise that people forfeit their privacy rights simply because they are overseas.** By arguing that non-British citizens are fair game, the UK sets a bad example to the rest of the world and provides justification to governments who spy on their own citizens and/or on the communications of British people resident in their country.

4.4.5 However, it is important to recognise that the impression created by the Snowden revelations is misleading in some key respects. It is not the case that GCHQ reads and listens to the communications of UK citizens en masse, as some media reporting has implied. GCHQ's mission is fundamentally foreign-facing. For that reason we welcome the

fact that the IP Bill includes a clearer statement to this effect, stipulating that the communications in question must be either sent or received by individuals located outside of the UK. This is an important safeguard against GCHQ's capabilities being deployed by a future government against the UK population. It also means that the collection of internet communications between an individual in the UK and a server based overseas (for example, a 'Google' search) is not within the intended scope of bulk collection.

4.4.6 We accept that there are very limited circumstances where a broader set of data has to be gathered in order to identify and collect necessary information on individual targets. For example, there is a clear national security case for identifying targets based in Syria who are conspiring with individuals in the UK to launch attacks here. The interception of those messages is a vital tool in stopping those attempts. It is not possible for the UK to approach the Syrian authorities to ask them to intercept the communications of suspects in Syria. The only alternative in these circumstances is to ask GCHQ to collect data in areas where hostile forces are known to be operating and to sift through it for the necessary intelligence.

4.4.7 **We therefore reject the idea that 'bulk' collection against overseas targets can or should be outlawed in its entirety.** To do so would ignore the fact that there are very limited circumstances where there are no alternatives and where the magnitude of the threat to the UK outweighs the intrusion into the privacy of a limited number of innocent citizens.

4.5 National Security Hotspot data

4.5.1 Given blanket prohibition does not makes sense, we must identify what legitimate 'bulk' collection looks like. **We believe that collection should be as geographically targeted as possible, with the objective of acquiring target information on potential national security threats where there is no realistic alternative means of obtaining the data. We call**

this 'national security hotspot data'. Such targeted bulk collection would be a significant reduction, and likely increase in effectiveness, of GCHQ's present activities.

4.6 Domestic data collection

4.6.1 The argument for national security hotspot data does not apply to the identification of suspects based in the UK. Here, the authorities can secure an interception warrant against any UK resident where they can demonstrate necessity and proportionality. Targeted communications data can be obtained direct from CSPs. The tools to identify and develop leads therefore exist in the UK where they may not overseas.

4.6.2 For this reason, **we cannot support the powers under section 94 of the Telecommunications Act 1984 (replicated in the IP Bill as 'bulk acquisition warrants'). This involves indiscriminate state collection and storage of phone call data on the entire British population.** It does, in effect, go beyond GCHQ's bulk collection powers and applies them to the domestic sphere. No compelling operational justification had been advanced for the UK equivalent of this database, which remains highly secretive. Liberal Democrats believe it crosses a red line into the blanket surveillance of the domestic population.

4.6.3 The same principle should apply to the collection of communications data by GCHQ as by-product of interception (known as 'related communications data'). Given that the role of GCHQ is to target communications where at least one of the parties is based overseas, the agency should be required to make every effort to avoid collecting either content or related communication data where both ends of the communication are in the UK. While it is not technically possible to prevent its inadvertent collection, **when UK to UK data is collected it should be deleted as a matter of course.**

4.6.4 Furthermore, additional safeguards are required for accessing communications metadata in certain situations, such as:

- To respect the additional public interest in the protection of confidential journalistic sources and correspondence between Parliamentarian and their constituents, in each case to safeguard whistle-blowers.
- For legally privileged communications and,
- Communications between individuals and medical professionals or religious advisers who are providing them with services

4.6.5 The current proposals from the Government fail to provide sufficient safeguards in any of these areas and **Liberal Democrats believe that there should be judicial authorisation in all these cases where such information is likely to be revealed (even if that is not the purpose) and that there should be notice of the application given to the person whose intercepted data is being accessed (except where this would prejudice an investigation) in order that the case for rejecting the application can be put.**

4.7 Criteria for collecting National Security Hotspot Data

4.7.1 The following criteria must be met before the collection of National Security Hotspot Data is approved:

1) The power to collect and access hotspot data should be limited to the intelligence agencies.

2) The Foreign Secretary should apply to a judicial commissioner for permission to put a warrant in place authorising collection to talk place.

3) The application must specify the national security requirements underpinning the warrant, based on the advice of the Joint Intelligence Committee. Collection can only take place for these purposes.

4) The judicial commissioner must be satisfied that the Foreign Secretary has considered and exhausted all reasonable alternatives, including diplomatic efforts and the use of formal data-sharing agreements with the government concerned.

5) The warrant must be limited in scope to the smallest practicable geographical area from which a threat to the UK emanates, in order to minimise collateral intrusion; the internet cables selected for interception must reflect these criteria.

6) The warrant should be limited to 6 months, renewable via a fresh application to the judicial commissioner.

7) All possible steps must be taken to avoid collecting the data of UK-based individuals who are not in contact with suspects in the area to which the warrant applies. Any such data, including metadata, which is inadvertently collected must be deleted as soon as it is identified as such.

8) Any data that is not relevant to investigations must be deleted within 30 days.

9) There must be no bulk collection of data that is not covered by the terms of these warrants.

10) The exceptional nature of these powers should be specified in statute.

4.8 Stronger oversight for hotspot data

4.8.1 **A small number of experienced lawyers should be appointed as 'public advocates' to sit alongside judicial commissioners when they make their determination on these warrant applications and renewals.** Their job will be to make the arguments for privacy and civil liberties which arise from the application, so that the judicial commissioner is not simply presented with a one-sided case.

4.8.2 **The Interception Commissioner and Judicial Commissioners should receive specific training** to allow them to scrutinise the use of hotspot data.

4.8.3 **The Privacy and Civil Liberties Board should conduct a biennial audit of the use of the intelligence agencies' use of hotspot data**, including an assessment of its value for money.

4.9 Application of these principle to Equipment Interference

4.9.1. **Liberal Democrats oppose 'bulk Equipment Interference' (EI or hacking) warrants as currently proposed in the Bill, as they are insufficiently targeted.** However, more targeted EI could be necessary and proportionate and in these cases the same principles as above should apply to EI.

4.9.2. The most important principle is that **UK intelligence agencies should not engage in EI where there are viable alternative means of obtaining the same information**, for example by working with equipment manufacturers and foreign governments.

4.9.3. EI can be significantly more targeted than bulk collection where it applies to the IT equipment of a known target, but it can also involve the creation of instability and security flaws in potentially safety-critical systems with implications for large numbers of users. **The regulations for EI should therefore require the government and the judicial commissioners to weigh up the operational benefits of the warrant against the collateral risks of proceeding.**

4.10 Encryption

4.10.1 Encryption provides a safe method for people to transfer information to each other. The most vaunted type of encryption, which is commonplace with secure websites

such as payment pages or personal banking, and with certain communications apps such as WhatsApp, is end to end encryption. End to end encryption means that only the sender and the recipient can read the message. When a message is sent, the application encodes the contents. The only application that can decode the content is the recipient – no one else has access to the encryption or decryption 'key'. Effective encryption of this type means that the ability to steal your information in transit is beyond the resources of most criminal gangs. This also means that government usually cannot decode such messages.

4.10.2 The Investigatory Powers Bill provides the Secretary of State with the ability to issue an order to a UK developer requiring them to provide backdoor access to their devices or software. It prohibits those issued with an order from disclosing the fact that it exists – so the government can have access to a huge array of devices and there would be no mechanism by which the public buying these devices can be informed. **Liberal Democrats believe that this is fundamentally wrong – encryption provides protection to individuals and if it is circumvented or broken, criminals and hostile foreign states can also breach security. When it comes to encryption, for the vast majority of users – privacy means security.** Instead Liberal Democrats **encourage the police and security services to make further use of alternative methods such as targeted equipment interference or targeted surveillance** to maintain their investigatory capabilities without undue collateral intrusion. Given the increased prevalence of end to end encryption, law enforcement has no choice but to develop new adaptation techniques.

Additional powers of the police and security services

5.1 Offline surveillance

Directed and intrusive surveillance

5.1.1 Outside the purely digital sphere, surveillance has always played a significant role. Both the police and security services have the powers to monitor suspects physically, or to place bugs or make use of existing systems such as CCTV. These kinds of surveillance are divided into two separate fields – directed surveillance and intrusive surveillance. Neither has such a large collateral footprint as the vast majority of aspects of online surveillance (with the possible exception of tightly targeted equipment interference), but there is likely to be a significant collateral impact (where innocent people's privacy is compromised).

5.1.2 Directed surveillance refers to the use of covert techniques to monitor an individual in public places. This may include tailing a suspect, taking photographs, tracking a vehicle, or making use of CCTV footage. It is considered to be less intrusive than 'intrusive surveillance' because it does not observe the most private aspects of life i.e.(those in a home setting) though there will be more collateral intrusion as surveillance will cover larger numbers of acquaintances and unrelated people. Warrants for this type of surveillance are approved by middle management level officials (e.g. a police superintendent or an inspector for urgent cases) and they are valid for 3 months.

5.1.3 Intrusive surveillance refers to the use of covert techniques to monitor an individual that is likely to reveal private information about a person, and is allowed under the Regulation of Investigatory Power Act 2000. Entering into someone's home or car in order to plant bugs or to intercept communications is allowed under legislation, such as under s.5 of the

Intelligence Services Act 1994 or Part III of the Police Act 1997. Equipment Interference or hacking is considered to be 'interference with property' although the use of malware to infect communication devices was never considered by parliament when the legislation was approved. This type of surveillance is highly targeted, but is likely to have a significant impact on collateral intrusion on other people (e.g. those who share a home). Warrants for intrusive surveillance are called 'Interception Warrants' and are issued by the Home Secretary under Section 5(1) of RIPA. In 2014, 2,795 warrants were issued – 1,705 for serious crime, 866 on national security grounds, and 224 on a combination.

5.1.4 While directed and intrusive surveillance remain preferable to any form of bulk or mass surveillance, we believe that because of its potential for collateral intrusion, it should **remain a measure of last resort.** Reports from the ISC suggest that owing to the considerable resources involved, these powers are used sparingly. We want to ensure that regardless of available resources or changes in bulk powers, they continue to be used cautiously.

5.1.5 Given that the establishment of Internet Connection Records is anticipated to cost at least £1 billion, we are confident that this funding could be spent more efficiently elsewhere. **We would therefore call for additional funding to be put towards strengthening the ability of the police and security services to undertake targeted surveillance and develop more community engagement strategies.**

5.1.6 On a related note, we are concerned about the sustainability of the Home Secretary alone being asked to approve over seven interception warrants every day of the year, in addition to their other duties. As with online surveillance, we believe that the appropriate body for approval of warrants in the majority of circumstances is a judicial commissioner rather than a Secretary of State. We also believe that the use of commissioners would enable more thorough examination of

warrants without unduly affecting other functions of the Home Secretary. We therefore **recommend that RIPA Section 5(1) warrants be approved by judicial commissioners.**

Covert Human Intelligence Sources (CHIS)

5.1.7 RIPA also provides for the authorisation of covert human intelligence sources. These are sources that establish or maintain a personal or other relationship with a person for the covert purpose of obtaining and disclosing information. This includes police informants and undercover officers.

5.1.8 In certain circumstances, directed or intrusive surveillance is either impossible to establish or maintain; in others, closer surveillance is required. For these scenarios, we believe that covert human surveillance may be the only option. However, we believe that the current arrangement where a senior officer (Chief Constable level) can sign off the use of an undercover officer is inappropriate. Given the likelihood that the use of undercover officers will result in greater collateral intrusion than, for instance, directed surveillance, additional safeguards are required. We would therefore **require time-limited judicial authorisation for the deployment of undercover officers by judicial commissioners and not senior police officers.**

5.1.9 Most recently, the use of undercover officers has been criticised for the role that they play in the lives of those they are monitoring. Mark Kennedy was a Metropolitan Police Officer who infiltrated a number of protest groups between 2003 and 2010. As a result of this disclosure, eight women said in 2011 that they were deceived into long-term intimate relationships by five officers who had infiltrated social and environmental campaign groups.

5.1.10 To prevent against this kind of abuse, we would **establish a code of practice for undercover officers that would routinely limit the activity in which they could engage,**

including sexual activity and the giving of evidence in court as their undercover personas.

5.2 Definition of Terrorism

5.2.1 Terrorism is defined in Section 1 of the Terrorism Act 2000.[17] Since 2000, several issues have been raised with this definition by, amongst others, the current and a former Independent Reviewer of Terrorism Legislation, Members of Parliament, and campaign groups. By and large, these concerns are related to:

- The use of the word 'influence' (acts designed to influence the government) in 1(b) by people who judge it to be too vague
- 1 (3) – any act or threat involving the use of firearms and explosives is regarded as terrorism regardless of motive
- The absence of a positive, rights-based statement such as those present in Canadian or New Zealand law.

5.2.2 Following Lord Carlile's report in 2008 and in line with David Anderson QC's recommendations in 2014, **we would reword section 1(b) of the Terrorism Act 2000 to remove 'influence' and insert 'compel, coerce or undermine'.**

5.2.3 In line with David Anderson QC's recommendations in 2014, **we would repeal section 1(3) of the Terrorism Act 2000.** We do not believe that the method of attack should be relevant to the classification of an action as terrorism (or not). Using a gun does not automatically make you a terrorist under the usual definition of the word. The use of a machete, release of poison gas, or use of a chemical or radioactive agent should be subject to the same requirements as the use of a gun or bomb.

[17] Section 1, Terrorism Act 2000 http://bit.ly/11Qowcv

5.2.4 We also recommend that a rights-based statement should be included in the definition of terrorism, designed to protect non-violent speech and action from the auspices of terror law. **We would therefore amend Section 1 of the Terrorism Act 2000 to include a new section (6)** – *For the avoidance of doubt, the holding or expression of a political, religious, or ideological thought, belief, or opinion, or participation in any protest, advocacy, dissent, strike, lockout, or other industrial action is not, by itself, a sufficient basis for inferring that the person has met the criteria of Section (1).*

5.2.5 We recognise that the combination of 'advancing a political, religious, racial or ideological cause' with the provisions relating to 'serious damage to property' would define Nelson Mandela's campaign against the South African apartheid government as terrorism. **Where insurgent groups use non-lethal force (such as industrial sabotage) and it is used against a repressive government that is, beyond doubt, non-democratic, we believe that these should not automatically fall within the definition of terrorism.**

5.2.6 We also **fully endorse David Anderson's recommendations on proscribed organisations in his 2012 report[18],** namely:

- That the government properly apply the existing law by prosecuting known members of proscribed groups and de-proscription if necessary
- That proscriptions are time-limited and subject to renewal after a set period
- To move to a two-stage statutory test for proscription which would introduce an additional requirement that proscription be necessary for purposes connected with the protection of the public from the threat of terrorism

[18] The Terrorism Acts in 2011, David Anderson QC http://bit.ly/1YIERXW

5.3 Terrorism and extremism measures

5.3.1 There are a number of powers in law which only apply to those arrested for terrorism. For instance, those arrested under the Terrorism Act 2000 rather than the Police and Criminal Evidence Act 1984 may be detained, subject to a judge's agreement, for up to 14 days. They may also be held incommunicado and refused access to legal representation where a senior officer has reasonable grounds for believing that such communication will lead to consequences including tampering with evidence, physical injury or the alerting of suspects. In this particular scenario, we would **require the routine reporting of instances where suspects are held incommunicado or without access to a solicitor as already happens in Northern Ireland.**

5.3.2 We are also concerned about the use of counter-terrorism or emergency powers beyond the uses for which they were intended. Most notably, the Anti-Terrorism, Crime and Security Act 2001 was used to declare Iceland's *Landsbanki* a proscribed regime in 2008, alongside countries such as al Qaeda, the Sudan, and Lebanon, so that Icelandic assets could be frozen. We do not believe that the use of counter-terrorism law for non-terror purposes is either justifiable or excusable. These uses undermine public confidence and affect our standing in the world.

Terrorism Prevention and Investigation Measures

5.3.3 We remain convinced that terrorism presents a threat that is complex and multifaceted that requires dedicated legislation in order to effectively police it. One such law is the Terrorism Prevention and Investigation Measures Act 2011.

5.3.4 We concur with David Anderson's assessment that "TPIMs are a necessary evil – I don't think anybody likes them very much."[19]. In all possible circumstances, we believe that

[19] The Today Programme, 22nd January 2014 http://bit.ly/22goR1i

charges should be brought and individuals should stand trial, rather than having their movements and interactions restricted. Occasionally this may not be an option in the short term. One of the key benefits of the TPIM system is that they can only be applied for one year, subject to a maximum one-year extension by a court. This measure reflects their intended use as a protective tool during investigation, and not as an alternative to conviction.

5.3.5 In addition to the changes made in 2015 (including the narrowing of the definition of terrorist related activity and requiring the TPIM subject to attend de-radicalisation interviews) we recommend:

- A TPIM cannot be imposed unless **the Home Secretary proves to a court on the balance of probabilities that a TPIM subject was involved in terrorism related activity.**
- **As soon as sufficient evidence is established that can be presented in open court, the individual should be prosecuted and the TPIM ended.**
- **A statutory bar should be placed on the use, as evidence for prosecutorial purposes, of, information that is provided during compulsory de-radicalisation interviews** – the lack of bar fundamentally undermines the need for openness in such a process.

Police Databases

5.3.6 In the Protection of Freedoms Act 2012, we ensured that biometric data such as DNA and fingerprints were not retained on people such as children, those found not guilty, and people who gave their DNA during the course of investigations. It also provided for individuals to apply to have their records removed from three databases – the National DNA Database, the National Fingerprint Database, and the Police National Computer.

5.3.7 Despite the 2012 Act, there remain other police databases, not subject to similar constraints. For instance, a photo

database established without notification of either the Biometrics Commissioner or the Home Office that holds over 18 million mugshots, with no regulation or oversight. This is simply unacceptable. Liberal Democrats would therefore **require all police and security services databases to be placed on a statutory footing – detailing the information involved; how it is collected, agglomerated, and stored; access; and purpose or use of the information.**

5.3.8 We welcome moves from the EU to implement rules on protection of data collected for law enforcement purposes. We would go further, however, to ensure that both the police and security services are bound by common principles in relation to the information they hold. There should be a **single set of stringent data protection rules including the sharing of police and security service data.** We would also require that **all information held by the police and security services (except by specific exemption) be subject to the same destruction timelines and procedures as DNA and fingerprints.**

5.3.9 Separately, the National Domestic Extremism and Disorder Intelligence Unit runs a central database called the National Domestic Extremists Database. This is formed of intelligence that is reported by surveillance teams at protests, rallies, and public meetings, and contains detailed files on individual protestors who are searchable by name. In addition, vehicles associated with protestors are tracked by automatic number plate recognition cameras. In line with our conclusion that non-violent extremism should not be criminalised, and understanding that if individuals had engaged in violent protest then they would be subject to ordinary criminal sanctions, **we call for the abolition of the National Extremist Database** and any similar police or security service databases that routinely hold information on private citizens without due cause.

Regulation of powers

6.1 Authorisation and oversight

6.1.1 Authorisation and oversight are key to the operation of the police and security services in a democratic society. The authorisation of warrants is a useful tool for protecting the freedoms of the public at large. They distinguish those being monitored from those not, and they place limitations on the investigation and its conduct. Oversight and review appear later, once the warrant has been approved and often once the investigation is complete. Ideally it is conducted by a disinterested body that has not had any involvement in authorisation or investigation.

6.1.2 The current oversight arrangements include the following bodies:

- the Intelligence and Security Committee
- the Interception of Communications Commissioner
- the Surveillance Commissioners
- the Intelligence Services Commissioner
- the Investigatory Powers Tribunal.

6.1.3 The **Intelligence and Security Committee** is a 9-member parliamentary committee that provides oversight of the use of investigatory powers by MI5, MI6, and GCHQ including oversight of operational activity and the wider intelligence and security activities of Government.

6.1.4 The **Interception of Communications Commissioner** is responsible for overseeing and reviewing online surveillance.

6.1.5 The **Surveillance Commissioners** are responsible for overseeing and reviewing the use of intrusive and directed surveillance, the use of CHISs, and protected electronic information by the police and public bodies such as the Food Standard Agency.

6.1.6 The **Intelligence Services Commissioner** is responsible for inspection and oversight of MI5, MI6, GCHQ, the MOD, and the warrant-issuing departments at the Home Office, the Foreign and Commonwealth Office, and the Northern Ireland Office.

6.1.7 The **Investigatory Powers Tribunal** (IPT) hears allegations of and provides the right of redress to those who believe they have been subject to wrongful interference with communications as a result of RIPA, and human rights claims. Cases can only be brought to the IPT by individuals not by one of the commissioners or by any organisation.

6.1.8 Clauses in the Investigatory Powers Bill Clauses create the Investigatory Powers Commissioner and the Judicial Commissioners, replacing the Interception of Communications Commissioner, the Surveillance Commissioners, and the Intelligence Services Commissioner. The Commissioners will be responsible for approving around 2% of warrants and for oversight of all warrants' approval. While we welcome the creation of a single oversight body, it remains a distinct concern that there is no distinction between approval and audit, and that Judicial Commissioners could be seen to be marking their own homework.

6.1.9 In line with the Royal United Services Institute's (RUSI) Independent Surveillance Review, David Anderson QC's A Question of Trust, and the Investigatory Powers Bill Joint Committee, **we would create a single, independent, public-facing oversight 'Commission' that would help to form a distinction between the approval and post facto audit elements of the oversight body.** This will present an opportunity to streamline the oversight landscape, to put all of the oversight responsibilities on a statutory footing, to bridge some of the identified gaps and address the overlaps.

6.2 Funding and Appointments

6.2.1 Under the Investigatory Powers Bill, the Secretary of State is still responsible for providing the Commissioner with the funding, staff and facilities that she considers necessary for the carrying out of the Commissioners' functions (Clause 204(2)). This is despite the Joint Committee suggesting rightly that it was inappropriate for the Secretary of State alone to determine the budget of the body which is responsible for reviewing the Secretary of State's performance.

6.2.2 In order to ensure independence and to comply with the modern international standard, **we would ensure that the Commission be responsible for determining the resources (including personnel) that they require to fulfil their role, and to determine their budget directly with the Treasury.**

6.2.3 We also believe that having Judicial Commissioners appointed by the Prime Minister is fundamental threat to the independence of the Commissioners. **We call for Judicial Commissioners to be appointed by the Judicial Appointments Commission in consultation with the Lord Chief Justice. Judicial Commissioners should also not be removed from office without the agreement of the Lord Chief Justice.**

6.3 Initiating Inquiries

6.3.1 One of the key weaknesses of the current system is the lack of ability of Commissioners to initiate thematic inquiries in response to public concern. Although they investigate the use of warrants, in the course of which they could identify persistent wrongdoing, they do not have the power to convert that into a fully-fledged inquiry. The Interception of Communications Commissioner's Office has raised the fact that it is difficult for them to produce these types of report without undermining core review functions – though both are key elements of ensuring robust oversight.

6.3.2 We would therefore ensure that **the 'Oversight' commission as established should have a clear mandate to launch inquiries into matters of public interest or areas of concern.**

6.4 Error Reporting

6.4.1 The Commissioners cannot currently notify individuals that their rights may have been violated unless they deem the conduct to be either 'wilful' or 'reckless', even in cases where there are widespread contraventions of a body's own internal procedures. The IPT requires no such assessment in order to investigate claims or even find in an individual's favour.

6.4.2 In order to enforce the powers individuals have over their own privacy and data, it is crucial to ensure that the error reporting provisions are clear and comprehensible and that individuals adversely affected are able to seek effective remedy. **We would therefore remove the requirement for Commissioners to deem that behaviour was 'wilful' or 'reckless' in order to notify individuals. We would ensure that the Commissioners have the power to refer matters or breaches directly to the IPT.**

6.5 Post notification

6.5.1 One of the key barriers to individuals appealing the contravention of their rights when it comes to surveillance not knowing that it has happened. Even with the removal of the wilful/reckless bar, we believe that there should be provision for citizens to be more routinely notified if they were subject to targeted surveillance and were completely innocent of any wrongdoing. This principle is called Post Notification. It is done routinely in Canada, for example.

6.5.2 In order to provide citizens with the information they need to hold their government to account, **we would incorporate the**

wording suggested by the European Court of Human Rights in 2007 into the Investigatory Powers Bill: "as soon as notification of targeted surveillance can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned."

6.6 Investigatory Powers Tribunal

6.6.1 In its current form the IPT upheld only 10 out of 1,673 complaints between 2000 and 2013. We believe that number of complaints to under-represent the underlying problem.

6.6.2 Part of the weakness of the IPT has been with the requirement that claimants have to prove harm (or 'material detriment') for compensation to be awarded – which is incredibly difficult in the case of bulk surveillance. We do not believe that harm is the salient issue when it comes to surveillance – we believe that the act of unlawful or unjust surveillance should be sufficient. **We would remove the requirement for claimants to the Investigatory Powers Tribunal to prove harm in order to obtain compensation.**

6.6.3 The IPT has also lacked the capacity for remedial action. If the case is proven, successful claimants only receive a letter saying that they were correct. **We recommend that the Investigatory Powers Tribunal has remedial power – the ability to award punitive damages, to direct the 'oversight' commission to undertake a full review of a body and its procedures, and to publish salient details of the case where appropriate.**

6.6.4 **We welcome in the Investigatory Powers Bill the provision for appealing a decision of the IPT on a point of law.** After more than a decade-worth of cases in which the Court of Appeal, the House of Lords and now the UK Supreme Court have each heard numerous appeals from closed proceedings in the High Court and the Special Immigrations Appeals

Commission, we can see no reason why the IPT's decisions should be insulated from challenge. In our view, the appropriate way forward would be to grant a right of appeal on points of law to the Court of Appeal.

6.7 The justice system: closed material procedures and statelessness

6.7.1 The justice system faces challenges, beyond oversight of government actions. For instance, there are Closed Material Procedures (CMPs) for civil claims conducted under the Justice and Security Act 2013, allow for closed hearings with special advocates in cases where individuals are suing the state and evidence that the state wishes to use would be harmful to national security.

6.7.2 The discussion within the party around CMPs in 2012/13 was extensive and conclusive. Conference overwhelmingly agreed on a number of occasions that 'the measures in Part II of the Justice and Security Bill will mean the courts system of the United Kingdom will provide neither justice nor security in cases involving allegations against the state of the most serious nature including torture, rendition, negligence of armed forces, malicious prosecution and false imprisonment.'

6.7.3 From the time the Act was passed to June 2015 (the most recent figures available), 16 requests were made for Closed Material Procedures. Only 5 were approved. These figures are low, and, of course, only for civil cases, but we do not believe that this mitigates the sense that justice behind closed doors and without the involvement of the claimant is not justice at all. We therefore **restate our existing party policy on Closed Material Procedures – that they are contrary to our values and purpose to 'build and safeguard a fair, free, and open society', and that Part II of the Justice and Security Act 2013 should be repealed.**

6.7.4 In recent years, revelations about the techniques employed by the police and security services such as those by Edward Snowden have undermined the argument that the provision of intercept evidence in court would publicise previously unknown technical capabilities. Intercept evidence, however, is already accepted in virtually every other EU and common law country, including the United States, France, Germany, and Australia. We do not therefore believe that the current ban is sustainable. **It has long been the policy of Liberal Democrats that intercept evidence should be allowed in court as it is in other countries, and we restate that here.**

6.7.5 In the Immigration Act 2014, the Home Secretary took on the power of being able to deprive a person of their British citizenship resulting from naturalisation, even if this left them stateless. Article 15 of the Universal Declaration of Human Rights declares that "everyone has the right to a nationality". To undermine such a fundamental tenet of international humanitarian law is unacceptable. We also believe that allowing provisions to be placed on naturalised citizenship over and above citizenship of origin is likely to have a negative impact on foreign-born British citizens, who rightly believe that their citizenship does not now enjoy the same status as that of somebody born in the UK.

6.7.6 Removing British Citizenship from someone while they are abroad does nothing to prevent terrorism. We also believe that given, in the intervening two years since this Act was passed, there has not been cause to enact this provision, it is an overreach of state power. **We would therefore repeal Section 66 of the Immigration Act 2014.**

Private information in company hands

7.1 Personal data

7.1.1 Recent years have been characterised by a huge growth in the amount of personal data collected by private companies. Some of this is information provided openly and willingly, such as where young drivers fit a 'black box' device to their car to monitor speech, braking, and the time of travel in an effort to reduce insurance premiums. More commonly, the provision of personal data is an automatic facet of a popular service, such as Apple's collection location data to promote advertising and to predict searches. Perhaps most importantly, the 'Internet of Things' (the network of physical objects that collect and exchange data without human interaction, such as thermostats like Hive or Nest) is providing an ever-increasing source of information indicative of habits.

7.1.2 The EU General Data Protection Regulation (GDPR) was passed in April 2016, came into force on 25 May 2016, and will take effect in May 2018. It updates the existing Directive to include, in the age of the internet and social media, the 'right to be forgotten'; access to private personal data; notification of hacking; security breaches; support for business with codes of practice and certification; and increasing penalties for data breaches in some cases up to 4% of a company's global turnover. We **welcome the strengthening of data protection in the digital age**, and believe that having a united approach across Europe is likely to have a positive impact for businesses that are not required to negotiate large numbers of differing regimes.

7.1.3 We particularly support the data protection principle that **personal data processed for any purpose or purposes**

shall not be kept for longer than is necessary for that purpose or those purposes.

7.1.4 Historically Liberal Democrats have aimed to raise awareness amongst consumers about what handing over their personal data could mean, thus hoping to reduce the willingness of consumers to part with their data. It is becoming increasingly clear, however, that particularly with younger consumers, ownership of private data is not a concern. The 2012 'Snooper's Charter' showed us that where there is resistance to government data collection, much of the same information is already held by large corporations and app developers without raising concerns. It appears that it is not data collection that concerns people, but who collects the data and what it is going to be used for.

7.1.5 **We would therefore require a clear and simple opt-in scheme for data sharing** – terms and conditions screens should not be seen as a valid alternative. **A fundamental part of the opt-in to data sharing is the ability to access a service even if consent for data collection is withheld.** In the modern age, the 'choice' over whether to use a service such as Facebook or even a device such as a smartphone is not a free choice, but we believe that the decision of whether or not to share personal data should be.

7.1.6 Extending the principle that data should be subject to the control of the individual to whom it refers, **we would require a clear and simple opt-in scheme for the sharing of data, with plain language explanations of who your data is being collected by and what it could be used for.** Terms and Conditions screens as they currently exist should not be seen as a valid alternative. We would also require that **companies who hold data on identifiable users contact that person once a year to provide them with clear and simple explanations of the data held on them**, perhaps in a standardized format, along with the ability to opt out of further data collection and the ability to remove existing data, unless

the organisation has a justifiable reason for keeping the data, such as preserving a contract.

7.2 Big data

7.2.1 An inevitable part of the data collection process is the use of data by the organisation collecting it for means beyond providing a service to the consumer. Most particularly, data can be used to analyse and influence consumption habits, sold on to additional companies, or gained in bulk to either append to existing databases or create new large databases. The last of these is known as 'big data' – extremely large data sets that may be analysed using modern technology to reveal patterns, trends, and associations. Big data includes internet search histories, financial information, meteorology, or purchasing information such as those gathered by using supermarket loyalty cards.

7.2.2 Once data is collected, its storage, use, and access are currently governed by the Data Protection Act 1998 (DPA) and in future by the GDPR. The DPA governs the processing of data on identifiable living people. The DPA allows an exemption for anonymised data. Anonymisation is the production of data in a form in which individuals cannot be identified, using reasonably likely means, even if combined with other databases – for instance, the number of patients who had a specific operation at a specific hospital. Anonymisation can be at the level of the individual but is more securely achieved by aggregating data. Pseudonymisation, on the other hand, produces disguised data on an individual-level basis – for instance a list of NHS patients in a local authority with their medical histories, but with names, addresses, NHS numbers, and dates of birth removed, where the data controller can readily re-identify the individuals if need be.

7.2.3 The concern with anonymised and pseudonymised datasets is that identifying characteristics may be reverse-engineered.

The DPA does not require anonymisation to be completely risk-free – companies must just be able to mitigate the risk of identification until it is remote. This is a reasonable requirement, but we believe that **is not sufficient. Additional consent should be sought from the consumer when data is collected, on an opt-in basis, for anonymised data to be shared. This should occur, in principle, for all instances where anonymised datasets are collected, used, sold, or shared.** For datasets such as the census, appropriate safeguards should be specified either in secondary legislation or in the relevant codes of practice.

7.2.4 The use of big data enables companies and government to better develop their services, drive innovation, and reduce the need for more costly and less accurate collection techniques such as surveying. We believe that **the use of big data should be defended.** However, it is important that big data can only be used to identify trends and not reverse engineer a picture of an individual. Bulk-level collections have inbuilt safeguards against individualising data, but pseudonymisation does not. We therefore believe that **the sale, sharing, and use of pseudonymised data should be restricted** so that clearly defined, time-limited, and organisation-limited consent is required.

7.3 Digital Bill of Rights

7.3.1 Our digital safety is, increasingly, fundamental to our security as individuals and as a nation. As a new framework for a digital age, **we welcome the EU initiatives which have led to the GDPR and the Directive on law enforcement data.** We look forward to the European Commission's proposals for a revised e-Privacy Directive.

7.3.2 We believe there is a need to regulate those data matters either outside EU competence or where flexibility is permitted in EU legislation. Our aim is to ensure that people have as many of the same rights to privacy in their telecoms and

online lives as they do in the offline world, whilst recognising the inevitable differences between the potential and inclination for data collection and processing.

7.3.3 **We therefore reaffirm our commitment to a Digital Bill of Rights that protects people's powers over their own data, that supports individuals over large corporations, and which preserves the fundamental neutrality of the Web.**

7.3.4 We will consult on the development of this Digital Bill of Rights, which should be shaped by the following principles:

- Online surveillance by the state must be the exception rather than the norm
- People have to same rights to privacy in their telecoms and their online lives as they do offline
- Personal data should, in principle, be subject to the control of the individual to whom it refers
- Everyone should be able to access, edit, or remove any online content which they themselves have created
- No public body is to collect, store or process personal data without statutory authority or explicit consent
- An open and neutral internet is essential for open government, good democracy, a strong economy, connected communities, and diversity of culture
- The right to free expression should apply online with no more restrictions than it does offline
- Consumers have the same rights to fairness and transparency online as they do offline
- Strong cyber-security is the basis of a strong digital economy
- Data that is created and maintained by government using public funds should be accessible to the public
- Children and young people should be able to enjoy the benefits of digital technologies without compromising their safety or privacy
- Anyone whose digital rights are breached has the power to complain to a competent authority.

Safe and Free – Policy Paper 123

This paper has been approved for debate by the Federal Conference by the Federal Policy Committee under the terms of Article 5.4 of the Federal Constitution.

Within the policy-making procedure of the Liberal Democrats, the Federal Party determines the policy of the Party in those areas which might reasonably be expected to fall within the remit of the federal institutions in the context of a federal United Kingdom.

The Party in England, the Scottish Liberal Democrats, the Welsh Liberal Democrats and the Northern Ireland Local Party determine the policy of the Party on all other issues, except that any or all of them may confer this power upon the Federal Party in any specified area or areas.

The Party in England has chosen to pass up policy-making to the Federal level. If approved by Conference, this paper will therefore form the policy of the Federal Party on federal issues and the Party in England on English issues. In appropriate policy areas, Scottish, Welsh and Northern Ireland party policy would take precedence.

Many of the policy papers published by the Liberal Democrats imply modifications to existing government public expenditure priorities. We recognise that it may not be possible to achieve all these proposals in the lifetime of one Parliament. We will set out our priorities across all policy areas in our next General Election Manifesto.

Working Group on Safe and Free

Note: Membership of the Working Group should not be taken to indicate that every member necessarily agrees with every statement or every proposal in this Paper.

Brian Paddick (Chair)
Francis Aldhouse
Alistair Carmichael MP
Tim Colbourne
Jeremy Hargreaves
Dr Evan Harris
Rosalind Huish
Sarah Ludford
Jonathan Marks
Justine McGuinness
Annabel Mullin
Mark Oaten
Zoe O'Connell
Umar Ramzan
Mo Saqib
Fraser Seifert
Paul Strasburger
Dr Jenny Woods

Staff:
Rachael Clarke
Jimmy de Jonge
Vinous Ali

Further copies of this paper can be found online at www.libdems.org.uk/policy_papers

The cost of not choosing our greener options

Every year for Conference, we spend around £30,000 and use over 2 tonnes of FSC recycled paper on printing copies of agendas, directories, policy papers, and reports to conference

Hundreds of our members are already selecting our Green Pack and our online-only options

Why not join them next tme and get your papers digitally at:
http://www.libdems.org.uk/conference_papers

Published by
Policy Unit, Liberal Democrats,
8-10 Great George Street, London, SW1P 3AE

Printed by
Bishops Printers, Walton Road, Farlington,
Portsmouth, Hampshire, PO6 1TR

ISBN: 978-1-910763-27-8

@libdems