Liberal Democrats

Liberty and Security

Policy Consultation Paper

Consultation Paper 124

Spring Conference 2016

Background

This consultation paper is presented as the first stage in the development of new Party policy in relation to liberty and security. It does not represent agreed Party policy. It is designed to stimulate debate and discussion within the Party and outside; based on the response generated and on the deliberations of the working group a full policy paper will be drawn up and presented to Conference for debate.

The paper has been drawn up by a working group appointed by the Federal Policy Committee and chaired by Lord Paddick. Members of the group are prepared to speak on the paper to outside bodies and to discussion meetings organised within the Party.

The Working Group has identified key questions it would like to discuss but we also welcome thoughts and suggestions on any other important issues not covered in this paper.

Comments on the paper, and requests for speakers, should be addressed to: Rachael Clarke, Policy Unit, Liberal Democrats, 8 - 10 Great George Street, London, SW1P 3AE. Email: policy.consultations@libdems.org.uk

Comments should reach us as soon as possible and no later than Friday, April 8th 2016.

Federal Policy Consultation Paper No. 124 ©February 2016

Contents

1. Introduction

1.1 The Preamble to our Party Constitution states that the Liberal Democrats exist to build and safeguard a fair, free and open society in which we seek to balance the fundamental values of liberty, equality and community and in which no-one shall be enslaved by poverty, ignorance or conformity. The values of freedom and openness are central to our identity as a party. Maintaining a free and open society requires an environment in which the public perceive themselves as safe from harm.

1.2 To prevent harm, we require a police service and security agencies. Recent tragedies across the world re-affirm this need, as do reports of the foiling of seven terrorist plots in the UK in the past year. While we acknowledge their necessity, the powers granted to these bodies must be proportionate. Parliament should have primacy in establishing limits on the powers of the security agencies. We need to secure the United Kingdom against those who wish to do us harm. But in granting the state disproportionate power, we risk losing a state worth securing.

1.3 As Liberal Democrats, our politics is driven by our values, but also by the evidence. It is increasingly clear that we cannot defeat terrorism through surveillance alone. Our focus should be to build trust in our communities. The Agencies should be our last line of defence. There is a battle of ideas to be won, and it will be won in our communities. Accordingly, building resilient communities, community policing and local intelligence should form a vital part of our fight against violent extremism. Excessive powers, on the other hand, encourage alienation.

1.4 This Policy Working Group will set out plans specifically designed to protect and enhance civil liberties in the UK, while maintaining and improving public safety and security. The Group’s final proposals will be informed by the debate around the government’s Investigatory Powers Bill (IPB), which is currently in the legislative process.

1.5 This Consultation Paper is organised around the main headings of our remit, which was set by the Federal Policy Committee.

2. Security Threats

2.1 Terrorism

2.1.1 We perceive the most severe threat to the United Kingdom at this time to be international terrorism. At the time of writing the Joint Terrorism Analysis Centre has assessed the situation as 'severe'. This is the second highest of five levels. It implies an attack is 'highly likely', without knowing about a specific attack.

2.1.2 In the UK, the terror threat derives primarily from violent extremists who self-describe as Islamic or Islamist. Current notable groups include Daesh (also known as ISIL), al-Qaeda, and various affiliates. In Northern Ireland there continues to be a significant risk of dissident republican attacks, though there have been no fatalities since 2012. Additionally far-right groups are becoming increasingly successful in inciting violence against the Muslim and Jewish communities, with hate crimes against both on the rise. One of our nearest neighbours saw a far-right extremist explode bombs killing eight people in Oslo and then shoot a further 69 at Utøya, Norway in 2011.

2.1.3 Returning 'foreign fighters' pose a particular risk as they may have been trained whilst overseas. Around 750 individuals have left to join Daesh or similar organisations. Of these, around half have returned. The devastating effect this training can have was visible in the highly co-ordinated attack on Paris in November 2015, principally carried out by European citizens who had trained in Syria.

2.1.4 A further threat arises from 'lone wolf' operators, or very small groups. These often independently develop a violent ideology and research attack methods, making them difficult for security agencies to track. Examples include the would-be Westfield bombers Mohammed Rehman and Sana Ahmed Khan. These attacks tend to be relatively unsophisticated, planned without significant external help, and executed over a short to medium-length timeframe.

2.1.5 Daesh, al-Qaeda and other extremist organisations conduct sophisticated propaganda campaigns, primarily via the internet. They seek to inspire others to join their cause, distribute propaganda materials and incite violence. Among the considerations we need to respond to is how to counter this incitement effectively, both online and offline.

2.1.6 Though the threat to the UK from terrorism is significant, it is not unprecedented. Seventy-five years ago, we faced an occupied Europe under Nazi rule. On the British mainland, there have been two victims of terrorism since the London bombings in 2005 – Fusilier Lee Rigby and Mohammed Saleem, who was murdered in Birmingham in 2013 by a far-right extremist trying to start a race war.

2.1.7 However, we note that the lack of successful attacks is not through a lack of attempts. That these have remained attempts owes much to the work of the police and security agencies (GCHQ, the Security Service or MI5 and the Secret Intelligence Service or MI6) in disrupting would-be attackers. According to Mark Rowley of the Metropolitan Police, since the 7/7 bombings, 50 UK-based attacks at various stages of preparation have been foiled. These varied in scope, from small-scale plots by 'lone wolf' operators to a sophisticated plot to blow up seven transatlantic airliners. The extent to which community intelligence, as opposed to investigatory powers such as interception, played a part in foiling these plots is not known.

2.2 Espionage and Cyber-espionage

2.2.1 According to publicly available information from the Security Service (MI5), at least 20 foreign intelligence services still actively operate against UK interests. Cyberattacks form a key tool in the arsenals of these services, due to the potentially large amounts of data that can be disclosed in a single breach.

2.2.2 A leaked US National Security Agency report in 2015 revealed that more than 600 high profile US corporate and government networks had been hacked by sources originating in China. Though these attacks did not directly target the UK, they did infringe on the data rights of a very substantial number of UK citizens who had data held with these companies.

2.2.3 Though there has not been an analogous release in the UK, reports make it clear the UK is subjected to a number of state-sponsored cyberattacks. As the Strategic Defence and Security Review 2015 notes, a growing number of states are acquiring advanced cyber-warfare capabilities. Furthermore, this threat is asymmetric, because the launch of a single successful attack will tend to be easier than the maintenance of a continuous successful defence.

2.3 Cross-border Crime

2.3.1 The UK's police forces operate within their own force boundaries, but criminals operate across national and international borders. While the National Crime Agency has a national remit (except in Northern Ireland), increasingly major crime involves international networks, particularly of drug and people smugglers. Co-operation with our international partners is increasingly vital, and must include dialogues and discussions about extending / opening up extradition powers.

2.3.2 Currently, we co-operate with European partner agencies primarily through the European Police Office (Europol). This agency provides law enforcement throughout Europe with tools and expertise, including allowing the exchange of information, intelligence analysis, and training in best practice. Co-operation with Europol has resulted in the dismantling of several cybercrime gangs and a number of major paedophile rings. In one such operation, 230 young victims of sexual abuse were rescued, 60 of them in the UK.

2.4 Cybercrime

2.4.1 Cybercrime is a growing threat, with 90% of large organisations and 74% of small businesses in the government’s 2015 Information Security Breaches Survey reporting a cybersecurity breach in the past year. Threats vary, and at the top end include Advanced Persistent Threats (APTs) and semi-organised groups such as Anonymous. These can bring significant technical expertise to bear on a specific target over a long period of time. Conversely, some threats are individuals who may "get lucky" against a random company, or who engage in relatively simple Denial-of-Service attacks targeting those against whom they bear a grudge.

2.4.2 A key problem with cybersecurity is the asymmetry between attack and defence. Launching a cyber-attack is a relatively simple process – defending against one is far more difficult. A single breach can result in the records of millions of people being leaked simultaneously. In one not atypical attack in 2015, the personal details of 156,000 TalkTalk users were compromised. This attack is believed to have been launched from the bedroom of a fifteen-year old boy. In 2013, Adobe had the details of 153 million customer accounts compromised in a breach. Some groups may also seek to blackmail companies by threatening to launch sophisticated Distributed Denial-of-Service (DDoS) attacks if a ransom, usually sizeable, is not paid.

2.4.3 Estimates for the cost of cybercrime are difficult to establish as organisations, whether public or private sector, are typically eager to cover up the fact that the breach occurred, fearing a loss of trust and potential legal claims. A 2011 survey by Detica suggested a total cybercrime cost to the UK of £27 billion in that year.

2.4.4 Cybercrime perpetrators are frequently located outside the UK, often placing them beyond the reach of prosecution. There is significant evidence to suggest that many Advanced Persistent Threats are state-sponsored, by foreign governments, and highly organised criminal gangs. Sensitive information gained from data breaches has been known to be passed on to companies who are in competition with UK businesses, and data on individuals used for blackmail.

2.4.5 So far, there is no publicly available evidence of a successful cyberattack on UK critical infrastructure. However, there are believed to have been successful attacks on infrastructure elsewhere. In 2010, a highly sophisticated attack using a computer 'worm', Stuxnet, is alleged to have destroyed a number of Iranian uranium enrichment centrifuges. The worm’s level of sophistication was exceptional, and commentators believed it required the resources of a state to create. However, it was released onto the Internet subsequent to the attack, and its designers are believed to have lost control of the worm. This is a key danger of cyberweapons – once in the public domain; they can attack unintended targets, or be adapted and controlled by other actors.

Questions

1. *How can Liberal Democrats endeavour to keep the debate around terrorism proportional to the threat level it poses?*
2. *How can we ensure policy around counter-terrorism is evidence-based?*
3. *In a world where the quantity of personal data held online increases rapidly, how can policymakers respond to data breaches?*
4. *How can we encourage the private sector to take better care of data they have been trusted with?*
5. *How can UK policymakers respond to the threat of state-sponsored cybercrime and cyber-espionage?*

3. Investigatory Powers

3.1 Background

3.1.1 The Liberal Democrats have a strong record of fighting for civil liberties, including blocking the Draft Communications Data Bill in 2012 (popularly referred to as the 'Snoopers' Charter').

3.1.2 In 2013, a series of disclosures by the former NSA contractor Edward Snowden revealed an unprecedented surveillance programme was being conducted by the US and UK security agencies. This included GCHQ's TEMPORA programme to tap into international fibre-optic cables and OPTIC NERVE, a program collecting images of Yahoo webcam chats in bulk.

3.1.3 Following the Snowden revelations, emergency legislation was passed to govern the powers of the police and security services. This Data Retention and Investigatory Powers Act (DRIPA 2014), has a 'sunset clause' and will expire at the end of 2016. DRIPA was subjected to a successful legal challenge in the High Court, which ruled elements of the Act incompatible with EU law. The case has now been referred to the European Court of Justice.

3.1.4 This has led to a wide-ranging debate around the necessary powers for the security agencies, culminating in the commissioning of three reports into investigatory powers. These are the Intelligence and Security Committee (ISC) Report, the Royal United Services Institute (RUSI) Report, and the report by the government's Independent Reviewer of Terrorism Legislation, David Anderson QC. A fourth report, by

Sir Nigel Sheinwald, has been completed but is not in the public domain.

3.1.5 The reports broadly agree the agencies require a licence to operate in the 21st century. The existing legislation governing their powers is anachronistic and not fit for purpose. They must have the tools they need to catch serious criminals and terrorists, but this must be within the bounds of what is proportionate and necessary in an open, democratic society.

3.1.6 The government released its response to these reports in the form of the Draft Investigatory Powers Bill in November 2015. A breakdown of the key issues is presented below.

3.2 Communications Data

3.2.1 There is substantial debate over the interception of communications data, also known as metadata. This concerns the external details of a communication, but not the content of the communication itself. For instance, in a phone call, this would consist of the caller, the recipient, the "cell" location where the call was made and received and the length of the call. It would not include what was said – this is the 'content' of the call itself.

3.2.2 Increasingly people are using the internet to communicate rather than fixed-line or cellular mobile phone communication. Establishing who communicated with whom and where they were at the time is far more difficult to establish when the internet is used, requiring the storage of massive quantities of data, including sensitive personal information. This information is not routinely kept by internet service or other communication services providers. In principle, it is argued, the police and the security services should be allowed to establish the same information currently available to them from traditional means of 'telephone' communication. Whether this can be done, technically and proportionally and without significant intrusion into personal privacy, is debatable.

3.2.3 It has been argued that some communications are by nature privileged and should be accorded a higher level of protection. In exercising their profession, lawyers, journalists, ministers of religion, medical professionals and Members of Parliament handle information of a sensitive nature. There is debate around whether their communications should be absolutely privileged and should never be intercepted, or whether there should be a higher legal test for intercepting them.

3.2.4 Technically, it is almost impossible to identify whether a particular 'packet' of data relates to a communication from the metadata alone. The information reveals the site being used – but not whether this is for communication, as opposed to browsing or shopping. To determine whether communication is taking place, internet service providers or the authorities would need to inspect content, which at the present time requires an interception warrant.

3.2.5 There is an argument that the interception of communications data is less intrusive than content. However, this argument generally takes a single piece of communications data and a single piece of content in isolation. Key to the intrusiveness of communications data is the gathering and analysis of it in bulk is far easier than the manual analysis of content by a person. Given the ever-increasing volume and types of communications data which can be collected, it is possible to rapidly build up a detailed picture of someone’s life.

3.3 Bulk Retention

3.3.1 A highly contentious part of the government’s proposals is the power to request that communication service providers acquire and retain ‘Internet Connection Records’ for up to a year, and to provide this data to the authorities on request.

3.3.2 This has attracted significant concerns from technology companies. Apart from the surveillance implications, they are worried about the costs and feasibility of retaining very large volumes of this data, and the costs of keeping it secure. The internet connection records of millions of people, containing a mountain of valuable information, would form a tempting target for hackers. This could lead to enormous privacy breaches if these internet connection records were made public by malicious third parties. There is a further question regarding whether retaining the internet connection records of very large numbers of UK citizens is proportionate.

3.4 Bulk Interception

3.4.1 Currently, the government proposes to continue with ‘bulk surveillance warrants’ which authorise surveillance as long as either the sender or recipient is outside the UK. This effectively provides legal footing for the TEMPORA programme described by Snowden. However, this poses significant practical challenges. In many cases, it is impossible to tell from the external communications data whether the originator or recipient is the UK, without examining the content.

3.4.2 Having determined the content, it is a question of trust that the security services would not use that information if it was useful to the police or the security services, or potentially politically, even if it was not for the purpose authorised in the warrant.

3.4.3 It is believed that such bulk interception is targeted based on initial intelligence rather than a fishing exercise involving the random targeting of innocent citizens' communications. The difficulty for the security services is providing enough information about the way they operate to reassure the public without telling criminals and terrorists how to avoid detection.

3.4.4 As part of the Anderson and ISC Reports, case studies were provided by the security services where bulk interception of communications data led to the identification of those involved terrorist activity. This included one case study (outside the UK but aided by GCHQ intelligence), where an attack was averted while the terrorists were *en route* to committing an outrage. Anderson notes as part of his report that GCHQ's case studies *"leave me in not the slightest doubt that bulk interception, as it is currently practised, has a valuable role to play in protecting national security"*. Unlike bulk data retention, the evidence suggests that the Agencies have gathered significant intelligence using bulk interception, and this has saved lives. Whether this is proportionate is a matter for us to decide on. Anyone's communications being read by the state without specific judicial authority is highly controversial.

3.5 Encryption and Equipment Interference

3.5.1 Given increasing use of encryption, 'Equipment Interference' (also known as 'Computer Network Exploitation') powers are proposed in the Draft IPB. This concerns hacking people's phones and computers.

3.5.2 There are two basic categories of encryption. In the first category, the 'key' is held by a third party, such as the company providing the encrypted service and shared with the sender and receiver of the communication. In theory such a 'key' could be handed over to the security services or stolen by hackers or hostile foreign government. The second category, 'End to end' encryption means only the sender and recipient of the communication possess the 'key' and not even the service provider can decipher what is being communicated.

3.5.3 End to end encryption is used by the vast majority of web services, as it allows for the secure exchange of information online, such as during an online banking transaction. However, it can also be used by terrorists or criminals to evade detection as their communications cannot be intercepted 'in-flight'.

3.5.4 To counter this, in the Draft IPB, the government gives the Agencies powers to commit equipment interference. This gives them the power to hack devices – to penetrate the security of the device and access the content once it has reached the target device and been decrypted. This is, arguably, the only way to access the content of communication on these devices. Obviously, the power for ‘equipment interference’ – state-sponsored hacking – is far more intrusive than passive surveillance. It involves actively exploiting or creating flaws in a device’s security, usually by ‘infecting’ the device with ‘malware’. Again, once created these means of hacking could fall into the hands of criminals or hostile foreign actors. That said, it is also a targeted form of surveillance – unlike bulk data collection which is less discriminating.

3.5.5 The Snowden revelations alleged sophisticated methods by which GCHQ and NSA operatives hacked into mobile phones and computers. This enabled them to read messages, listen to conversations and even activate cameras and microphones. These are highly intrusive and controversial techniques.

3.5.6 Whilst most equipment interference is targeted towards specific suspected individuals or groups, the draft Bill allows for all devices in a certain area to be targeted. For instance, if the police service is aware that a target is in a particular area, they would be able to harvest information from all devices in that area, regardless of whether they had any connection to the target or not. There is an argument that this is necessary on a practical level, as individuals seeking to evade surveillance may use multiple methods of communication and change these rapidly. However, there are concerns over these ‘bulk equipment interference’ warrants, due to the intrusiveness of these powers.

3.5.7 It is possible for all cellular communication within a particular cell to be intercepted, using a device known as an IMSI catcher. This effectively replicates a mobile phone mast, but records all traffic passing through it, revealing the subscriber data of all individuals in an area. These devices can also intercept and block messages. There have been allegations in the British press that IMSI catchers have been used by the Metropolitan Police in London, potentially invading the privacy of tens of thousands of people without their knowledge. This again raises the question of innocent people's communications being intercepted without judicial authorisation, and without the knowledge of the individuals concerned.

Questions

<u>Investigatory Powers</u>

6. *Should the security agencies be accorded different powers from the police?*
7. *What agencies, if any, should be able to access communications data?*
8. *Is all communications data equal? If not, what should the hierarchy be?*
9. *Does the proportionality argument mean that bulk data interception can never be used? Can any safeguards ever mitigate the use of bulk data interception?*
10. *Should the communications of journalists, lawyers, ministers of religion, elected representatives and medical professionals be privileged? If so, should this be absolute, or subject to a higher threshold for interception?*

<u>Data Retention</u>

11. *Should communications data or internet connection records be retained by communication service providers?*

12. *If there is a proven national security need, should government be able to mandate the retention of communications data?*
13. *Can encryption adequately mitigate the risk of data retained by communications service providers being hacked by third parties?*
14. *If required for operational reasons, for what length of time should communications data be retained? Is the government's suggested 12 months reasonable?*

Authorisation of warrants

15. *What data, if any, should the police and security agencies be permitted to access without external authorisation?*
16. *What should the authorisation process for investigatory powers look like? Should this process be different for criminal and national security investigations?*
17. *Can a dual-authorisation model, in which the decision of a Secretary of State is reviewed judicially, provide an appropriate safeguard?*

Equipment Interference

18. *Speaking theoretically, if the state has two means at its disposal to gather information, the first being less intrusive but conducted in bulk, and the second being more intrusive and targeted, which is the greater infringement on liberty?*

4. Regulating Investigatory Powers

4.1 Closed Material Procedures

4.1.1 The Justice and Security Act 2013 introduced Closed Material Procedures (CMPs, commonly referred to as ‘Secret Courts’) – civil courts in which a defendant is represented not by their appointed legal counsel, but by a special advocate with security clearance who can view the evidence. They argue the case behind closed doors. The appellant is informed of the gist of the evidence against them, but not the detail.

4.1.2 In the past, proponents argue, the security services, unable to divulge sensitive intelligence in open court, were unable to contest the claims. Now the judge is able to hear both sides of the case, albeit in closed session.

4.1.3 Closed Material Procedures have seen very little use – in the government’s latest published statistics to June 2015, the Home Secretary has made a total of nine applications for CMPs, five of which have been granted.

4.1.4 The debate over the introduction of CMPs was hard-fought in the party. Conference passed several motions calling for our Parliamentary teams to oppose them, and a number of party members publicly resigned. It is not our intention to rehearse here the arguments on either side, but clearly CMPs provided a significant break from earlier practice, and given the role of intelligence and security in their establishment, and their function in holding government intelligence collection to account, their use must be considered.

4.1.5 In our 2015 General Election manifesto, we committed to identifying practical alternatives to the use of closed material procedures within the justice system, including the provisions of the 2013 Justice and Security Act, with the aim of restoring the principle of open justice.

4.2 Authorisations for Surveillance

4.2.1 The UK is the only member of the 'Five Eyes' group of signal-intelligence sharing powers (the UK, USA, Canada, Australia and New Zealand) that has surveillance warrants authorised by the executive. All others have judicial involvement or approval.

4.2.2 Anderson argues that given the increasing need for international co-operation, particularly in seeking information from USA-based giants such as Facebook and Google, the UK should fall into line with other members of the 'Five Eyes' alliance. Conversely the Intelligence and Security Committee argues that authority should be given by ministers who can be held to account for their actions in Parliament. Although Secretaries of State are prohibited by law from discussing individual warrants, they could be held to account for the quantity of warrants being issued, for example.

4.2.3 The government's proposals in the Investigatory Powers Bill leave the decision with Ministers, the decision being 'judicially reviewed' by specially appointed judges. The nature of the 'judicial review' is altered – from the normal criterion as to whether the decision of the minister was ‘unreasonable’, to the test applied in Human Rights cases where proportionality also has to be considered.

Questions

<u>Closed Material Procedures</u>

19. *How can the justice system best deal with the need to admit evidence requiring security clearance?*
20. *Can the use of Closed Material Procedures ever be justified? If so, what safeguards should be put in place?*

<u>Authorisations for surveillance</u>

21. *Can a dual-authorisation model, in which the decision of a Secretary of State is reviewed judicially, provide an appropriate safeguard?*
22. *Should all warrants be authorised judicially, or are there certain warrants that should remain with the relevant Secretaries of State?*

5. Regulation of Police and Security Services

5.1 The Investigatory Powers Tribunal

5.1.1 The Investigatory Powers Tribunal (IPT) was established by the Regulation of Investigatory Powers Act 2000. It is currently the only judicial body to which complaints about the three Agencies can be directed.

5.1.1 The IPT has been criticised for its lack of transparency. Since its creation, it has upheld a total of 10 complaints – out of a total of 1,468 complaints made. In making decisions, the claimant’s lawyers are excluded. The Tribunal has no power to force the government to disclose any document. Additionally, it is a purely reactive body. It does not audit the conduct of the agencies and cannot begin its own investigations; instead it has to wait for referrals or external complaints.

5.1.2 The Investigatory Powers Bill creates a new, domestic right of appeal to the Investigatory Powers Tribunal on a point of law. This is a welcome development – but it still does not alter a fundamental question – how can an individual appeal against state surveillance if they are never told they have been spied on?

5.2 User Notification

5.2.1 One proposal to mitigate increasingly intrusive state powers is the concept of ‘user notification’. If an individual is placed under surveillance, they are informed of this fact a set amount of time after the surveillance has ceased. This is a qualified right, which can be delayed if the security services demonstrate that the individual continues to pose a potential threat, despite active surveillance having ceased.

5.2.2 User notification hence allows the individual to challenge the state's surveillance of them, by informing them of this fact and opening the possibility of appeal. However, there are concerns from the security services, worried it may compromise their ability to investigate suspects. There is a further question around when the duty to disclose would be triggered.

5.3 An International Framework

5.3.1 The intelligence agencies and security services must have the trust of the ordinary people they serve. Revelations from Snowden showing states have been working together to circumvent national laws has undermined this trust. Going forward, an international framework for surveillance could be developed – focused around principles that could set the global gold standard. This recognises the fact that states must work together to counter terrorism and proliferation.

5.3.2 The Five Eyes have already disclosed information sharing agreements and arrangements (Mutual Legal Assistance Treaties), as they relate to international law enforcement and national security measures but not intelligence sharing. However, we do know that highly-integrated signals intelligence (SIGINT) sharing arrangements do exist between these developed powers.

5.3.3 Mutual Legal Assistance Treaties (MLATs) are law enforcement tools that allow States to request another country to locate wanted individuals, issue warrants, share evidence, obtain testimony, freeze bank accounts, or repatriate seized assets. MLATs are frequently applied to the sharing of online information. And, like intelligence-sharing agreements, an overarching template for co-operation is filled in with a detailed set of 'below-the-waterline' rules and regulations. However, unlike informal intelligence-sharing agreements, MLATs are subject to international treaty law.

5.3.4 These processes are often cumbersome and prone to time delays; nevertheless they provide legal clarity for Communications Service Providers and global technology companies. In 2014, The UK Government appointed Sir Nigel Sheinwald as Special Envoy on intelligence and law enforcement data sharing. Sheinwald conducted a report into this area. Whilst this report has not been published in full, a summary has been released. This called for greater data sharing between like-minded countries, where threats are often shared; reform of the US/UK MLAT; the building of a new international framework and called on Government to improve transparency in this area.

5.4 Future-proofing

5.4.1 The law has a tendency to be several steps behind technological developments. Therefore, it is important that new legislation contains the means to update the law as technology evolves. However, it is equally important to avoid loosely drawn legislation being used to provide legal cover for activities it was never intended for. One can see this particularly in section 94 of the 1984 Telecommunications Act. This tiny section of an unrelated Act provided the legal basis for many of GCHQ's surveillance programs over the last thirty years.

Questions

The Investigatory Powers Tribunal

24. *What powers should the Investigatory Powers Tribunal have?*

25. *What reforms are required to the IPT to ensure it is able to effectively hold the Agencies to account?*

26. *How can we best provide redress to those who have been subjected to unlawful surveillance?*

User notification

27. *Would bringing in user notification hamstring the ability of the police and security services to do their work? If so, is there a means to prevent this?*

28. *Should there be a right to be notified if you have been placed under surveillance? If so, at what degree of intrusion should the duty to disclose be triggered?*

29. *What rules should be put in place around the notification of individuals who have been placed under surveillance?*

30. *Should a 'right to be notified' be qualified (able to be overruled completely) or absolute (only able to be delayed)?*

International Framework

31. *Do you think there should be an international framework governing surveillance laws and international co-operation?*

32. *If such a framework is created, what key principles should underpin it? What do you think this should look like?*

Future-proofing legislation

33. *Should there be a statutory duty for surveillance legislation to undergo periodic review?*
34. *Should surveillance legislation contain a 'sunset' clause, meaning it requires renewal, to keep the powers of the agencies in the public eye?*

6. Protecting our Data

6.1 Data Protection Legislation

6.1.1 Most of the data protection legislation that is in force today was passed before 2000, the primary piece of legislation being the Data Protection Act 1998. Since then, new technology has revolutionised the way we live and communicate. Smartphones, social media, WiFi, 4G, GPS, and other web platforms and content have heralded a shift in the vast majority of our communications from the offline to the online world. Proposed new pan-European legislation is in the legislative process, including tougher penalties for data breaches which could see firms being fined up to 4% of their annual turnover.

6.1.2 While the growth of the internet has enormous socio-economic benefits, it has also left people open to exploitation and misuse of their personal information by criminals, commercial interests, and public authorities. Liberal Democrats have called for a Digital Bill of Rights, to protect the privacy and rights of citizens on the internet. This would enshrine in law the fundamental right of the citizen to have ownership of their personal data, and control who has access to it.

6.2 Commercial Exploitation

6.2.1 The increase in communications has meant a considerable increase in the amount of our personal data which is online. Bulk personal datasets, involving data on millions of customers, have become increasingly valuable due to their value in targeting online advertisements.

6.2.2 The use of new technologies creates a personal digital footprint encompassing our movements, social connections, personal characteristics, behaviour and even our private thoughts. Once created, this footprint can offer valuable insights to private companies interested in targeting consumers with tailored advertising, as well as to law enforcement and intelligence agencies seeking to detect and prevent illegal activity. The advent of 'Big Data' is accelerating this trend. While there are enormous potential benefits from the analysis of large data sets (for example, in increasing our understanding of illness and improving public health, or in tailoring advertising more closely to consumers' needs), there are also many difficult issues to navigate around privacy and consent.

6.2.3 There is an imbalance of information in many of our online interactions. Users effectively 'give up' their information – personal data, browsing history, map requests and other usage data – in return for the free provision of a service such as Facebook or Google. However, they are informed of little around what the company does with their data. This can include the analysis by the company in question of information most users see as private. For instance, Google clarified in 2014 that its systems scan all emails sent to and from its servers, and that the data from this was used to generate more targeted advertising.

Questions

Data Protection

35. *How can we give citizens control of their data in a practical manner?*
36. *How should we police data rights violations?*

Commercial exploitation of personal data

37. *Should Liberal Democrats challenge the commercial exploitation of personal data? If so, how?*

38. *How should policymakers respond to the phenomenon of bulk personal datasets?*

7. Engaging Communities

Terrorism Act 2000 (S1 – Interpretation)

(1) In this Act “terrorism” means the use or threat of action where—
(a) the action falls within subsection (2),
(b) the use or threat is designed to influence the government or an international governmental organisation or to intimidate the public or a section of the public, and
(c) the use or threat is made for the purpose of advancing a political, religious, racial or ideological cause.

(2) Action falls within this subsection if it—
(a) involves serious violence against a person,
(b) involves serious damage to property,
(c) endangers a person’s life, other than that of the person committing the action,
(d) creates a serious risk to the health or safety of the public or a section of the public, or
(e) is designed seriously to interfere with or seriously to disrupt an electronic system.

(3) The use or threat of action falling within subsection (2) which involves the use of firearms or explosives is terrorism whether or not subsection (1)(b) is satisfied.

(4) In this section—
(a) “action” includes action outside the United Kingdom,
(b) a reference to any person or to property is a reference to any person, or to property, wherever situated,
(c) a reference to the public includes a reference to the public of a country other than the United Kingdom, and
(d) “the government” means the government of the United Kingdom, of a Part of the United Kingdom or of a country other than the United Kingdom.

(5) In this Act a reference to action taken for the purposes of terrorism includes a reference to action taken for the benefit of a proscribed organisation.

7.1 Defining Terrorism and Extremism

7.1.1 The definition of terrorism in British law is argued to be too broad. The definition provided by the Terrorism Act 2000 has the potential for significant ‘creep’ beyond its intention.

Under the current regime, journalists or bloggers could be subject to anti-terrorism powers if they publish something the authorities deem ‘dangerous to life, to public health or public safety’. As David Anderson noted in his review of powers, a campaigner objecting to vaccination on religious grounds could be sanctioned under anti-terror laws, if the government makes the case that his actions are likely to damage public health. Voicing support for him, equally, would be a terrorist crime.

7.1.2 The Government recently published its latest counter-extremism strategy, which they claim builds on working with communities to prevent and identify radicalisation. A Bill on countering extremism will shortly follow and is set to include measures such as new Banning Orders for extremist organisations, Extremist Disruption Orders to “restrict the harmful activities of extremist individuals” and Closure Orders, “a new power for law enforcement and local authorities to close down premises used to support extremism”.

7.1.3 Extremism is currently defined 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.” In order for the new powers granted by the Counter Extremism Bill to be effective and enforceable, a legal definition will need to be created. This raises a number of sensitive issues, a few of which David Anderson QC highlighted in his 2015 Terrorism Acts Report: the range of political and religious views whose expression falls within the definition of extremism; whether that definition includes views critical of the Government; and whether the definition of extremist activity is intelligible, clear and predictable.

7.2 The Impact of Counter-terrorism Strategies

7.2.1 Section 44 stops, which allowed the police to stop and search any person or vehicle within a specific area without reasonable suspicion, ceased in 2012. However, other counter-terrorism measures continue to be used disproportionately. Schedule 7 of the Terrorism Act 2000, allowing authorities at ports and airports to stop and search for up to nine hours without charge, does not even require a reasonable suspicion that someone is engaged in terrorist activity. 32,000 examinations took place in 2014/15. Of these, 1,300 resulted in a detention.

7.2.2 Studies show that these stops have a significant negative impact on Muslim communities. As one study noted, ‘For some Muslims, these stops have become a routine part of their travel experience’. This is to the extent that an interviewee in one study noted the first question their friends asked returning from a trip abroad was ‘did you get stopped, and what did they ask you?’ Individuals perceived as Muslim in appearance can equally be affected by this.

7.2.3 There is an operational case for stop and search as a targeted tool. As the case of Richard Reid, the would-be ‘shoe bomber’ shows, there may be cause to question passengers. But subjecting communities to disproportionate, intrusive searches has the potential to alienate many of them. It furthers a perception terrorist groups seek to exploit – that of ‘otherising’ particular communities as suspect.

7.3 Counter-extremism Strategy

7.3.1 One solution to countering extremism is to be found in empowering communities. A counter-narrative must be created to the allure of violent extremism. However, this has not always been done well in the past. The government's PREVENT strategy, to prevent young people from being drawn into violent extremism, has come under significant criticism. One senior police officer has stated publicly that it is perceived by many in the Muslim community as a tool to spy on them.

7.3.2 PREVENT, it has been argued, has a misguided view of the radicalisation process. It assumes previously 'normal' individuals become radicalised, and then turn violent as a result of this radicalisation. In fact, many of the individuals involved in terrorism are known to the criminal justice system. They are often violent before their views become extreme. At least three of the Paris attackers were known to the police, two having spent time in prison for robbery.

7.3.3 Counter-extremism initiatives must be transparent. Basic information on the various CONTEST counter-extremism initiatives, such as which organisations and individuals are receiving funding, should be publicly available. The impact of counter-extremism projects, and how this impact is assessed, should be subject to public scrutiny.

7.3.4 Government must be clear about the process of the Channel programme; meant to support individuals at risk of being drawn into violent extremism. Channel is opaque; at least two internal evaluations have been undertaken but neither has been published. For communities to trust the government, the government must be transparent in its dealings. Additionally, government must be clear which individuals and organisations it is consulting on counter-extremism initiatives.

7.3.5 Oversight must be extended into counter-extremism strategy. To this end, there should be an independent reviewer of Counter-Extremism legislation, in an analogous role to that of David Anderson QC for surveillance.

Questions

Terrorism, extremism and radicalisation

39. *How should we define terrorism? How do we distinguish it from non-violent extreme views?*
40. *How should extremism be defined legally?*
41. *Should legal remedies be used to counter extremism?*
42. *How can we counter online radicalisation?*
43. *Where should we draw the boundary between protected free speech, unlawful hate speech, and incitement to violence?*

PREVENT and counter-extremism strategies

44. *What is the evidence for the PREVENT strategy? Do we know if it works?*
45. *What has the impact of PREVENT been? How should it be modified?*
46. *How can we ensure PREVENT and similar programs have people with the right skillsets for the job?*
47. *How can we ensure there is transparency around community outreach programs?*

48. *How should we engage with extremists? How should we engage with those who have renounced extremism?*
49. *How can we help communities fight terrorism?*

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

Printed by: Sarum Colourview LTd, Unit 8 Woodford Centre, Lysander Way, Salisbury, Wiltshire, SP4 6BU.

Layout and Design by Christian Moon.

ISBN: 978-1-910763-18-6