Freedom Restrained?
Public Protection, Risk and Policing
20 - 22 April 2018
Briefing Document
Research Associate: Dr Francesca Menichelli
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Foreword</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Introduction: what do we want to be protected from?</strong></td>
<td>3</td>
</tr>
<tr>
<td></td>
<td><strong>Section 1: Police power and terrorism</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>1.1 Stop and Search</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>1.2 14-day detention</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>1.3 Temporary exclusion order</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>1.4 Border Controls</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>1.5 Terrorism Prevention and Investigation Measures (TPim's)</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td><strong>Section 2: The Investigatory Powers Act 2016 and the regulation of electronic surveillance</strong></td>
<td>9</td>
</tr>
<tr>
<td></td>
<td><strong>Section 3: Safeguarding mechanisms for child protection</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3.1 DBS and enhanced screening</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>3.2 Safeguarding Children Boards</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td><strong>Section 4: The management of violent and sexual offenders for public protection</strong></td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>4.1 Multi-Agency Public Protection Arrangements (MAPPA)</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>4.2 The violent and sexual offenders register (ViSOR) and disclosure schemes</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td><strong>Section 5: Key issues to consider</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>5.1 Discrimination</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>5.2 Media</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>5.3 Privacy and proportionality</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td><strong>Section 6: Conclusion</strong></td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>References</td>
<td>21</td>
</tr>
</tbody>
</table>
We live in times of heightened public anxiety over risks in private and in public space, but how far should we go in terms of curtailing the freedoms we enjoy to ensure our security? This is a fundamental question for society as whole, yet there is little time to reflect on it – not least for those involved in policing, who must respond to pressing needs and threats. The expansion and strengthening of counter-terrorism legislation is one area in which the police if affected by the tension between liberty and security, as is the tightening of safeguarding procedures in respond to sexual abuse.

Given the complexity of this issue, and the strong and conflicting feelings and opinions it can provoke, I am delighted that our forthcoming conference, Freedom Restrained? Public Protection, Risk and Policing, will provide a rare opportunity for informed discussion and reflection on the role the police play in protecting citizens from harm, and how this should be balanced against safeguarding fundamental human rights. As well as being the latest in a long series of Cumberland Lodge police conferences, it is also a core part of the Lodge’s ongoing work on social cohesion. We hope that the conference will lead to innovative thinking with practical outcomes for all involved, and we will ensure that any findings are followed-up and disseminated more widely through the conference report and a seminar in Westminster later in the year.

We are grateful to our Research Associate, Dr Francesca Menichelli, Lecturer in Criminology at the University of Surrey, for writing this briefing document, which is designed to help you prepare for the conference. It is also available for others to use, and can be downloaded from our website: https://www.cumberlandlodge.ac.uk/learning-resources/freedom-restrained-public-protection-risk-and-policing-conference-briefing.

Our grateful thanks also to KBR, Police Mutual, and the Dawes Trust for their generous support. As well as helping us meet the overall running costs, this year we have been able to provide bursaries to enable several doctoral students and officers nominated by the College of Policing and the Police Now scheme to attend. As well as widening the range of participants and perspectives, their involvement will hopefully help ensure longer term outcomes from the conference.

I look forward to see you at Cumberland Lodge.

Canon Dr Ed Newell
Principal, Cumberland Lodge

Slido

This briefing document is designed to help you prepare for the conference and spark key questions to consider.

We will be using Slido throughout the conference, and at the end of each session there will be time for Q&A. We would encourage you to send us any questions that you would like the speakers to comment on by sending them to us in advance via Slido https://www.sli.do/ using the event code: #Q129. Please include the name of the session or speaker that your question is relevant to.

Alternatively, you can email any questions to Hannah Breeze, Programme Administrator hbreeze@cumberlandlodge.ac.uk.
introduction: what do we want to be protected from?

In troubling times, fear spreads, trust dwindles, and walls go up. Many questions thus arise. Where should we draw the line between legitimate requests for protection and intrusive security measures? How do we tell the difference between proportionate responses to existing threats and risks, and unacceptable attempts at curtailing societal and individual freedoms? And who should make such judgments? These important and complex questions are at the heart of the upcoming Cumberland Lodge Police Conference, ‘Freedom Restrained? Public Protection, Risk and Policing’.

This briefing document presents a summary of key issues to inform conversations and debates during the conference. While by no means exhaustive, it provides a roadmap that, it is hoped, will help delegates navigate what is a vast and continually changing landscape. The document is structured as follows: this introduction is followed by Section 1, which describes the powers police have in their fight against terrorism; Section 2 provides an outline of the Investigatory Powers Act 2016 and the rules it has introduced for electronic surveillance; Section 3 considers the safeguarding of children; Section 4 outlines mechanisms for the management of violent and sexual offenders in the community; in Section 5 key issues are offered for consideration; and a brief conclusion is presented in Section 6.

Before attempting to explore the interplay between public security and individual freedoms, we need to consider how risks have changed and, just as importantly, how society’s awareness of and responses to these risks have changed as well. This briefing, therefore, focuses on the following areas: counter-terrorism, safeguarding and child abuse. Both are indicative of heightened public anxieties over risks in private and in public spaces, and reflect the significant shifts that have taken place in the ways in which society perceives and responds to specific threats. A variety of elements are at play in each of these areas, some of which are specific and others more general.

counter-terrorism

The movement away from organised groups, such as Al-Qaeda, towards the model of independent sleeper cells favoured by IS has meant that military operations in foreign countries are no longer considered the first line of response to terrorist attacks. Instead, it is now commonly agreed that national security services, in general (and counter-terrorism, in particular) are the governmental agencies best equipped to deal with radicalised individuals who may be planning attacks inspired by ideologies, as opposed to being directed by larger terrorist groups.

It is reasonable to believe that the threats posed by individuals who are radicalised online and then go on to commit attacks are likely to play a part in compounding widespread feelings of insecurity and of being under threat. A YouGov poll conducted on behalf of the BBC on public perceptions of the threat of terrorism is significant in this regard (YouGov, 2016). The pollsters were able to conclude that the perceived threat of terrorism in the UK constantly increased between 2010 and 2016, and that while respondents thought it was highly unlikely that they would be directly affected, 84% believed that ‘an attack on British cities and other targets is likely’ (YouGov 2016). Sadly, the question proved to be prescient, and in the course of 2017 the UK was attacked several times — in Manchester, Westminster and Finsbury Park — as were France, Spain, Belgium and other European countries. In response to these fears and attacks, the British government passed legislation specifically targeting terrorists and terrorism-related activities. Some of the measures resulting from such efforts curtail the rights of suspects in significant ways; for example, extending the maximum duration of pre-charge detention to 14 days, from the customary 72 hours. As will be shown in this briefing, this is potentially problematic and raises important questions on where the balance between security and due process should rest.
With regard to the safeguarding of children, the movement has been towards increased transparency, better support for victims, and a greater willingness to shed light on crimes (often long kept in the dark) that preyed on the especially vulnerable. When the extent of the abuse that Jimmy Savile was able to carry out for decades was finally brought to light in 2012, outrage erupted, prompting the launch of an Independent Inquiry into Child Sexual Abuse (IICSA).

More recently, similar revelations on the scale of the abuse inflicted on vulnerable girls in Rotherham, Oxford, Rochdale and elsewhere have forced councils to review their actions and admit to their failings. On a practical level, this institutional wave of self-questioning has pushed councils to learn from their mistakes and has resulted in efforts to strengthen existing lines of communication and accountability to ensure that issues are tackled as soon as they arise.

The working culture of the organisations involved was also identified as part of the problem, as it was accepted that a more rapid and decisive response was greatly impeded by 'a lack of knowledge and understanding around a concept [of Child Sexual Exploitation (CSE)] that few understood and where few knew how it could be tackled, but also of organisational weaknesses which prevented the true picture from being seen' (OSCB 2015: 2). In its national inspections on child protection, Her Majesty's Inspectorate of Constabulary (HMIC) equally acknowledged that 'the police must reassess their approach to child protection' (HMIC 2015), and that the combined scale of historical and current sexual abuse suffered by children necessarily calls for different sets of skills on the part of police officers, and new ways of working for forces as a whole. With regard to this, it is hoped that the conference will offer delegates an opportunity to have open and challenging conversations on how organisational cultures and working practices will have to change to meet the needs of the most vulnerable members of society.

The shifts we have identified are still in progress and the resulting legislative and operational landscape is in a state of constant flux. This is why we believe that it is necessary, at this point in time, to critically consider the responses that society has put in place in these areas, and to see if, and to what extent, they uphold and reflect the values of justice, equality and fairness, and what could or should be done if they do not.

‘Where should we draw the line between legitimate requests for protection and intrusive security measures? How do we tell the difference between proportionate responses to existing threats and risks, and unacceptable attempts at curtailing societal and individual freedoms?’
In recent years, a number of terrorist attacks and incidents have taken place in the United Kingdom. Authorities claim that an even larger number of plots have been foiled thanks to the work of the police and security services. This section analyses the specific powers that police forces have in responding to terrorism, and provides an outline of the wider legislative framework that regulates these powers.

### 1.1 Stop and search

Police forces have a variety of different powers to stop and search individuals: ‘Most, but not all, of these powers require an officer to have reasonable grounds for suspicion that an unlawful item is being carried’ (College of Policing 2017). Within the scope of this briefing, two types of Stop and Search (S&S) will be considered: the powers governed by Code A of PACE (Police And Criminal Evidence Act), and powers accorded to the police by the Terrorism Act 2000, Sections 43 and 47a.1

In Code A, police officers can stop a suspect only if they have reasonable grounds to believe the person is carrying a weapon, stolen property, drugs, or something that could be used to commit an offence. Possible exceptions to this requirement necessitate authorisation by a senior police officer and this can only be given if there is suspicion that the person is carrying a weapon, or that ‘incidents involving serious violence may take place’ (Home Office 2014a: 5). Before being searched, a suspect must be told what the police are expecting to find and the reason why they are being searched. Periodically, controversies erupt regarding S&S and how it is used to target minorities in a disproportionate manner. According to Home Office data, ‘people from an ethnic minority background are 3 times more likely to be stopped and searched than White people’ (Home Office 2017a), while the likelihood increases seven-fold for black people.

The power to S&S in relation to terrorism and related offences is regulated by Sections 43 (search of persons) and 47a (searches in specified areas or places) of the Terrorism Act 2000. With regard to the former, a person can be stopped only if there are reasonable grounds to believe they might be a terrorist, and in order to obtain evidence in support of this suspicion. Any possession or material acquired during S&S can be retained by the police. According to the powers granted by the 2000 Act, an officer from any of the police forces across the UK has the authority to S&S a suspect anywhere within the UK. Searches can also be carried out in ‘specified areas or places’ if there is reasonable suspicion that an act of terrorism will take place. The authorisation to carry out the search is necessary in order to prevent the act. Vehicles located in the specified area can also be searched, along with the drivers, passengers, and any content found in the cars or carried by any persons inside the car. The same applies to pedestrians. Crucially, as per Section 47.5, the power to S&S can be ‘exercised whether or not the constable reasonably suspects that there is such ‘evidence’.

Unfortunately, there are limited amounts of data specific to Sections 43 and 47a, as most police forces do not produce separate statistics for terrorism-related and PACE-regulated S&S. For Section 43 stops, data are available only for the Metropolitan Police Service from 1 April 2009 to 31 March 2017 (House of Commons Library 2017: 8). Within this timeframe, 5,635 stop and searches were carried out in London, with around 5% resulting in an arrest. The ethnicity of the people stopped can be broken down as follows: 40% White, 29% Asian or Asian British; and 11% Black or Black British. No S&S has been carried out to date for Section 47a.

---

1 Section 47a was added to the Terrorism Act 2000 to replace Section 44, repealed with Protection of Freedoms Act 2012.
1.2 14-day detention

While pre-charge detention cannot be longer than 72 hours in normal criminal cases, a special regime is in place for terrorism-related offences, which means that detention can last up to 14 days. Since its introduction in 2001, this specific measure has been the object of constant revision. Until 2003, pre-charge detention could last 7 days at most, but this was extended to 14 days until 2006. Between 2006 and 2008, the maximum length was doubled to 28 days, before returning to the current limit of 14 days.

According to House of Commons data, ‘of the 1,855 people arrested under section 41 of the Terrorism Act 2000 since 11 September 2001, the majority (90%) have been detained for fewer than 7 days; 739 people (40%) have been held for less than one day, and 925 (50%) for between one and seven days. Only 11 people have been detained for longer than 14 days, 10 in 2006/07 and one in 2007/08. Six people were detained for the 28 day maximum period in 2006/07’ (House of Commons Library 2017: 17). For the year ending in March 2017, 60 people were placed in pre-charge detention, as per Section 41 of the Terrorism Act 2000. Of these, 36 (60%) were eventually charged. The same period also ‘saw the highest number of terrorism-related arrests (304) in any financial year on record since the data collection began in September 2001, an increase of 18% compared with 258 arrests in the previous year’ (Home Office 2017b: 4). Overall, 75% of arrests were linked to international terrorism, while domestic terrorism was mentioned in 16% of cases. With regard to the ethnicity of suspects, there was a 66% increase in the number of white people arrested for terrorism-related offences, compared to the year ending in March 2016. In absolute terms, this translates to 37% of people arrested identifying as white, up from 26% in the previous year.

1.3 temporary exclusion order

The on-going conflicts in Syria and Iraq have attracted a number of individuals who, for a variety of reasons, have decided to take part in armed battle in these wars. The phenomenon is consistent and widespread. Research on foreign fighters (FF) estimates that between 2014 and 2015 as many as 300,000 combatants from 104 countries could be found in the region. The International Centre for Counter-Terrorism (ICCT) in The Hague has calculated that around 4,000 foreign fighters are from member states of the EU, with a little less than 3,000 coming from just four countries: Belgium, France, Germany and the United Kingdom (Van Ginkel and Entemann 2016). Research from the ICCT indicates that around 30% of foreign fighters have returned to their countries of departure, and widespread concerns exist around the potential security threat that these individuals represent.

British authorities have said that at least 500 British nationals could be linked to terrorist activities in Syria and Iraq (Home Office 2014b). While powers already existed to prevent foreign nationals and naturalised Britons from returning to the UK after having participated in terrorist or terrorist-related activities abroad, these did not apply to individuals who only held British citizenship. As stripping these people of their citizenship would make them stateless, the government introduced a new power within the 2015 Counter-Terrorism and Security Act that was designed to temporarily exclude such people from returning to the United Kingdom. Temporary Exclusion Orders (TEOs) are imposed by the Secretary of State, can last up to two years, and can be renewed. If such an order is issued, the individual concerned can only return to the UK after making contact with the authorities. Once in the UK, they can also be subject to specific requirements, such as taking part in de-radicalisation activities. Other measures can also be imposed by either MI5 or the Police, while the Crown Prosecution Service can consider whether or not there are grounds to press criminal charges. It is possible for an individual who receives a TEO to seek a judicial review of the decision that was made to issue the order.
Data from the Transparency Report on Disruptive and Investigatory Powers published by the government in February 2017 show that no TEOs had been issued at the time of publication (HM Government 2017). In January 2018, the Minister of State for the Home Office revealed that while no TEOs had been issued between 2015 and the publication of the 2017 report, they had been used ‘several times’ since, with ‘the next Annual Transparency Report, due for publication in Spring 2018, confirm[ing] how many times the power has been used during 2017’ (HC Deb 05 January 2018 c 121325).

1.4 border controls

Schedule 7 of the Terrorism Act 2000 allows police officers to stop, question and, if necessary, detain, people travelling through borders, ports, airports and international rail stations in order to determine if they might be involved in the commission or preparation of terrorist acts. No grounds of suspicion or prior knowledge are necessary for someone to be stopped, and the person can be detained for up to six hours. They can also be required to hand in their property, including electronic devices with their passwords, which can be retained for up to seven days.

The Home Office publishes quarterly and annual data on the operation of police powers under the Terrorism Act 2000. In 2017 ‘a total of 16,349 persons were examined under this power in Great Britain, a fall of 16% compared with the previous year, and a fall of 73% since the data were first collected in the year ending 31 December 2012, when 60,127 persons were examined under Schedule 7. Since the data collection began in 2012 we have seen average year on year falls of 23%’ (Home Office 2018: 21).

The same criticisms levelled at the power to stop and search can be raised here. In terms of ethnicity, 66% of people stopped under Schedule 7 are members of minority communities. While this is flagged by advocacy groups, such as Liberty, as being seriously problematic and proof of the discriminatory nature of British anti-terrorism legislation, the government has argued that this criticism misses the point as the proportion of those being stopped under Schedule 7 should not be compared to the distribution of ethnic groups in the general population, but rather to the ethnic breakdown of terrorists (HM Government 2017: 17). The Supreme Court of the UK shares this view, arguing that ‘there is also no substantial risk of these powers being used on a racially discriminatory basis. The statistics show that the exercise of Schedule 7 powers is proportionate to the terrorist population, considering the sources of the terrorist threat, which travels through UK ports’ (Supreme Court of the United Kingdom 2015).

1.5 Terrorism Prevention and Investigation Measures (TPims)

Terrorism Prevention and Investigation Measures (TPims) were introduced in 2011 to replace the controversial control orders established by the Prevention of Terrorism Act 2005. TPims are civil preventative measures and can be used only when the prosecution or deportation of individuals thought to be involved in terrorist activities is not possible. A higher test than control orders has to be satisfied for TPims to be issued, and they are designed to be less disruptive to an individual’s ability to maintain a normal routine: ‘A key objective of the [2011] Act was to introduce a more focused regime with increased safeguards for the civil liberties of those subject to the measures, which still protected the public from the risk of terrorism’ (Home Affairs Committee 2016: 1).

TPims are approved by the Home Secretary and can last for up to two years. They can include overnight residence requirements, electronic tagging, and specific limitations on whom the person subjected to it can meet, or where they can go. Overseas travel is also prohibited. However, as opposed to control orders, TPims do not preclude the use of computers, mobile phones or the Internet for work and study.
In 2015, TPims were strengthened and ‘[p]roof of involvement in terrorism-related activity to the civil standard of proof is now needed, not merely reasonable belief, placing a somewhat higher burden on the state to impose a TPIM’ (Fenwick 2017). In their new incarnation, once again TPims now include, as control orders once did, the possibility of forced relocation up to 200 miles away from an individual’s usual place of residence, along with the requirement to attend de-radicalisation activities.

The latest data available reveal that in October 2017 there were six individuals placed under TPims in the UK, with ‘one notable trend [being] the reduction in the number of measures issued against foreign nationals over the years with a contrasting increase in those issued against British Citizens’ (House of Commons Library 2017: 23).

‘The Home Office publishes quarterly and annual data on the operation of police powers under the Terrorism Act 2000.

In 2017 ‘a total of 16,349 persons were examined under this power in Great Britain’

The Investigatory Powers Act 2016, which received Royal assent in November 2016, completely reorganised the legal framework which regulates the investigatory powers of intelligence agencies and law enforcement with regard to the interception of communications and the access to communications data. The rules in place before the passing of the Act were dispersed across several legislative texts. This made it particularly difficult to understand what powers the authorities had and what existing safeguards existed, and also complicated any meaningful attempts at public oversight over these powers and the understanding of how authorities had actually been using them. The 2016 Act was aimed at rectifying this. First, it set out, and in some measures expanded, the surveillance powers of intelligence agencies and law enforcement. Second, it strengthened and expanded the safeguards applicable to the exercise of these powers, introducing a new authorising regime for authorities seeking to engage in electronic surveillance, along with the concurrent establishment of a new public body tasked with keeping the public and Parliament informed on how these powers are used.

The Act also covers the interception of communications, which can take two different forms: it can be targeted, meaning that it is directed at a specific individual or group of individuals; or it can be bulk, which means that large volumes of data are collected and stored for a set amount of time, with the possibility for law enforcement agencies to go back to them and look for possible patterns and connections.

Two types of data can be intercepted: communications data (or metadata) and content data. Metadata is information relating to the context in which a digital communication has taken place. For example, in the case of a phone call, the phone numbers, location of the person who made the call (as well as that of the recipient) and the length of the call itself are all considered metadata. Important conclusions can be drawn from this kind of information. In the case of terrorist activities, knowing whom a suspect called, and how often and for how long, can give us important clues as to the structure of their network.

However, in order to find out what the people within that network said to each other, content data needs to be collected. As per the letter of the Act, nine agencies can apply for a warrant to intercept communications: MI5, SIS, GCHQ, the Ministry of Defence, Her Majesty’s Revenue and Customs, the National Crime Agency, the Police Service Northern Ireland, Police Scotland, and the Metropolitan Police Service. A warrant can be granted only if interceptions are carried out for one of three specific purposes: in the interest of national security; for the prevention or detection of serious crime; and for the safeguarding of the economic wellbeing of the UK (for national security).

A novel aspect introduced by the Act is the requirement for communication service providers (CSPs) to retain their customers’ Internet connection records (ICR) for one year. ICR are ‘records of the internet services that have been accessed by a device’ (Home Office 2015a: 1) and are essentially a list of the websites that have been visited via a given laptop, smartphone or computer. This provision was harshly criticised by privacy campaigners and civil rights organisations during the passage of the Bill through Parliament, and is the reason why the Act is now colloquially known as the ‘Snoopers’ Charter’. What may have been lost in the public debate surrounding this aspect of the Act is that ICR show the service that was accessed (e.g. the BBC website), and do not provide any additional information as to what the user looked at within that specific service (e.g. the news stories clicked on across the BBC website). This means that it is not possible to reconstruct an individual’s complete Internet browsing history with ICR. An extensive, and at times surprising, list of agencies can access ICR without a warrant, including, among others, the Department of Health, the Department for Transport, the Department for Work and Pensions, and the Food Standards Agency.
Along with organisations from the civil society, concerns over the legality of the ICR provision have also come from the European Court of Justice, which in December 2016 reiterated that the generalised retention of personal data is not proportional and is therefore unlawful. As a consequence, in early 2017 it appeared as if the requirement for CSP to retain ICR had been shelved.

In December 2017, following a public consultation, the Home Office published five codes of practice relating to different powers set out in the Act, although six were originally supposed to have been released. According to the Home Office, ‘the sixth code of practice, concerning communications data, will be published for consultation at a later date. The Retention of Communications Data Code of Practice 2015, published under the Regulation of Investigatory Powers Act (RIPA), will remain in place until otherwise stated’ (Home Office 2017c: 3). It remains to be seen what might happen to this provision if, or when, the European Court of Justice no longer has any jurisdiction over the UK.

With regard to safeguards, the 2016 Act has established a ‘double lock’ authorising regime that requests for warrants to carry out interceptions must undergo. Initial authorisation must be given in person by a Secretary of State, typically the Home Secretary, and then be approved by a judicial commissioner serving on the newly established Investigatory Powers Commission (IPC). Taking over the responsibility from the Interception of Communications Commissioner’s Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISComm), the IPC also oversees the wider use of interception powers, monitors compliance with the Act and provides information to the public on the use of these powers by the authorities. As of yet, the Commissioner has not published his first annual report, and data from previous years are of limited significance (as the double-lock regime established by the Act was not in place).

‘This provision was harshly criticised by privacy campaigners and civil rights organisations during the passage of the Bill through Parliament, and is the reason why the Act is now colloquially known as the ‘Snoopers’ Charter’.
section 3: safeguarding mechanisms and child protection

In recent years, revelations over the scale of historic and more recent abuse suffered by children throughout the UK have renewed concerns over the suitability of the mechanisms in place for the protection of minors, and more generally vulnerable individuals, and on how swiftly authorities act to protect those in their care. In this section we will cover two of these mechanisms: DBS and enhanced screening, and safeguarding children boards.

3.1 DBS and enhanced screening

The Disclosure and Barring Service (DBS) is a non-departmental public body established in 2012 as a result of the merger of the Criminal Records Bureau and the Independent Safeguarding Authority. It is tasked with carrying out background checks on prospective employees, on behalf of organisations working with children or vulnerable adults, so as to ensure that recruitment practices are safe and unsuitable individuals are excluded from certain professions. During the course of a person’s employment, the DBS also has the responsibility of investigating any referrals that the employer might decide to submit to them. Safeguarding concerns should normally be raised when a person has caused significant harm (in the widest sense of the word) to a child or vulnerable individual, or when there are reasons to believe that the person’s conduct might put them at risk of future harm. Failure in the duty to refer is an offence, and any individual failing to submit a referral without any valid justification can be fined for up to £5,000.

There are three different types of checks that the DBS offers to employers: standard checks, enhanced checks, and enhanced checks with barred lists. A standard check shows all the spent and unspent convictions a person might have, along with cautions, reprimands and final warnings. An enhanced check builds on this and includes all the above, together with any additional information held by the police that is considered to be relevant for the job the person has applied for. Finally, an enhanced check with barred lists shows whether the applicant is currently on one or both of the two lists maintained by the DBS (the Children’s Barred List and the Adults’ Barred List), and therefore automatically excluded from any paid or voluntary activity involving either group.

Understandably, the judgement of the officer charged with providing additional information to be included in the enhanced check is of crucial importance and guidance has been issued in support of this task. As per instructions issued by the Home Office (2015b), the police should only provide additional information if this is relevant for the prescribed purpose and if the information itself can be traced back to a credible source. The age of the information, along with the age of the applicant at the time and their conduct since, should also be taken into consideration and appropriately balanced with an understanding of the seriousness of the offence. Generally, the older the information, the harder it would be to make a case for its relevancy and therefore inclusion in the enhanced check, although in the case of very serious offences age should not be a determining factor.

The guidance explicitly recognises the potential impact that disclosures can have on the private life of the applicant. In order to be compatible with Article 8 (right to private life) of the European Convention on Human Rights, the disclosure must therefore be legitimate, necessary and proportional, meaning that the relevancy and seriousness of the information justify the impact on a person’s privacy, that the disclosure is being pursued for a legitimate purpose, and that there are no other practical options available that allow the pursuit of the same aim in a less intrusive manner. In light of the complexity of the task, the guidance dictates that ‘the reasoning in reaching a decision [should] be fully and accurately recorded in each case’ (Home Office 2015b: 3).
‘The guidance explicitly recognises the potential impact that disclosures can have on the private life of the applicant. In order to be compatible with Article 8 (right to private life) of the European Convention on Human Rights, the disclosure must therefore be legitimate, necessary and proportional.’

The National Audit Office (NAO) has very recently published a report that is highly critical of the attempts that have been made to modernise the DBS (NAO 2018). In 2009, the Home Office launched a transformation programme with the intention of reducing the cost and increasing the efficiency of safeguarding services. Despite only being established in 2012, the DBS was included in the programme in order to make it cheaper and more efficient. This is of crucial importance as, while being sponsored by the Home Office, the DBS is financially dependent on customers paying for disclosure certificates. Looking at how the new and cheaper update service was launched by the DBS, NAO concluded that an appropriate business case had not been made prior to the launch of the service to find out what the potential demand for it was. Additionally, the report argues that the DBS still has no idea why the take-up by users has thus far been much lower than expected, which has resulted in the expected savings not being delivered. Despite the problems with the update service, NAO agrees that the safeguarding service provided by the DBS is still effective.

Data contained in the NAO report show that ‘in 2016-17: some four million disclosures were issued, of which some 260,000 (6.1%) contained information potentially relevant to safeguarding; there were one million subscriptions to the update service, for which 2.6 million status checks were made (of which 0.1% indicated new information was available); and the lists of people barred from working with children or vulnerable adults contained some 64,000 individuals as at 31 March 2017’ (NAO 2018: 8). Recent DBS data show that between April and September 2017 the DBS issued almost 2.1 million disclosure certificates, with 92% of those being for enhanced screenings. In the same period, 3,061 referrals were received. The latest data available shows that as of the end of August 2017, a total of 65,794 individuals are placed on the two barred lists maintained by the organisation (DBS 2018).

Looking beyond the data, another problematic aspect also comes to light. In its report, NAO stressed how ‘there are no checks on how employers use information provided by DBS. DBS’s role is to process the safeguarding information that the police hold and provide this to employers on request. Employers are responsible for complying with legislation when they make employment decisions. There is no check on what employers have done with the information provided by DBS. Government does not know how many people this information prevented from working with children or vulnerable adults’ (NAO 2018: 8). This information is particularly troubling in light of some of the wider criticisms that have been levelled at the role vetting and screening play within child protection policies in the UK. Among others, a report for think tank Civitas argues that far from protecting children, these practices have ingenerated a widespread culture of suspicion that is damaging inter-generational relationships at a fundamental level, and is hampering the activities of the voluntary sector (Furedi and Bristow 2010). While these kinds of statements are extremely hard to verify with recourse to data, some volunteering organisations have claimed anecdotally that one of the reasons for the current shortage of volunteers is indeed the requirement for the DBS checks to be carried out on all applicants (Hope 2008).
3.2 Safeguarding Children Boards

In its most recent iteration, the government’s approach to children’s safeguarding is described as ‘child-centred and coordinated’. On a practical level this means that local arrangements must be underpinned in all their aspects by two overarching principles: first, that ‘each professional and organisation should play their full part’; and second, that services should be ‘based on a clear understanding of the needs and views of children’ (HM Government, 2015: 9). Established by the Children Act 2004, Local Safeguarding Children Boards (LCSB) play a key role within these arrangements, making sure that the services being provided locally to children are effective and accountable.

Set up in every local authority, LCSB are multi-agency bodies which play a strategic role in the planning and evaluation of child protection services in their local area. Bringing together a series of relevant agencies, they aim to coordinate the safeguarding efforts of all partners, while ensuring the overall effectiveness of actions being taken. The 2004 Act lists the statutory functions of LCSB. They develop children safeguarding policies in relation to: thresholds of intervention; the recruitment, training and supervision of people working with children and the investigation of allegations against them; the wellbeing of children who are privately fostered; and the cooperation with children’s services in neighbouring authorities. They also monitor and assess the effectiveness of children’s services policies, carry out serious cases reviews, and participate in the planning of services. LCSB do not provide any service directly, nor do they commission any themselves. However, they obviously work very closely with children’s services in their area.

Membership of the board is also defined in the Act and is designed to bring together a wide range of institutions, including the NHS, local government, probation and prison (if there are facilities which ordinarily detain children). The police representatives on the Board for each of the partner agencies should have senior roles in their home organisations, and be able to commit them on policy issues and decisions made by the Board. The chair of the Board is independent and is thus able to hold to account all partner agencies and organisations. In addition, the chair is required to work closely with the Director of Children’s Services for the local area.

The Board must publish an annual report on its activities and on the overall effectiveness of children’s safeguarding services in the area, with particular emphasis on the assessment of performance, the areas flagged for improvement, and what is being done to solve problems and weaknesses. Additionally, the Board should also conduct regular evaluations of its own effectiveness and the effectiveness of partners’ responses to cases of CSE.
Upon their release, violent and sexual offenders present authorities with a series of difficult problems to solve. On one hand, the statistics on reoffending rates do not make a particularly uplifting read in terms of the chances of someone successfully reintegrating into their community. On the other hand, victims, their families and the public at large might be very worried at the prospect of someone returning to live among them after spending time in prison for a particularly serious offence. However, once they have served their time, offenders are likely to return to their communities, and authorities have to find strategies that can serve several purposes at the same time: decreasing the chance of reoffending, providing tools and opportunities to facilitate reintegration, and ensuring that society is adequately protected. Several instruments have been developed to meet these, at times competing, ends.

### 4.1 Multi-Agency Public Protection Arrangements (MAPPA)

Established by the Criminal Justice Act 2003, Multi-Agency Public Protection Arrangements (MAPPA) are a set of statutory arrangements developed to assess and manage the risks posed by certain types of offenders once they have been released from custody. Each MAPPA brings together three agencies with responsible authority status: the police, probation, and prison service. There are also a number of other organisations which all have a duty to cooperate: Youth Offending Teams, Local Housing Authorities, Health Trusts and Authorities, Adult Social Services and Children’s services, and Job Centre Plus. In England and Wales, each MAPPA is coterminous with the 42 police force areas. Comparable arrangements are in place in both Scotland and Northern Ireland.

Three categories of offenders are managed through MAPPA: Category 1 consists of registered sexual offenders who, upon release, need to register with the police for any period of time between 12 months and life, depending on the facts and circumstances of their crime; Category 2 consists of violent offenders who have been sentenced to a custodial sentence longer than 12 months; and Category 3 consists of other dangerous offenders who are deemed to pose a risk to the public.

Intersecting this categorisation of offenders are three different levels of management available to which offenders can be subjected, depending on the level of inter-agency cooperation necessary: ‘Ordinary agency management level 1 is where the risks posed by the offender can be managed by the agency responsible for the supervision or case management of the offender. This does not mean that other agencies will not be involved, only that it is not considered necessary to refer the case to a level 2 or 3 MAPPA meeting’ (Ministry of Justice 2017a: 45). Level 2 cases are cases where the offender is considered as posing a high or very high risk of serious harm, cases that require the active coordination of more than one agency, or cases that no longer require level 3 management. This ‘should be used for cases that meet the criteria for level 2 but where it is determined that the management issues require senior representation from the Responsible Authority and Duty-to-Co-operate agencies. This may be when there is a perceived need to commit significant resources at short notice or where, although not assessed as high or very high risk of serious harm, there is a high likelihood of media scrutiny or public interest in the management of the case and there is a need to ensure that public confidence in the criminal justice system is maintained’ (Ministry of Justice 2017a: 45).

The latest data available for the year 2016-2017 show that as of 31 March 2017 there were 76,794 MAPPA-eligible offenders in England and Wales. Of these, almost 72% are Category 1 offenders, while the overwhelming majority across all categories (around 98%) is managed at level 1. Since 2008-2009, when the current recording standards were established and data were therefore directly comparable, the numbers of offenders in Categories 1 and 2 have almost doubled (+170% and +180%, respectively), while Category 3 offenders have almost halved (Ministry of Justice 2017b).
4.2 the violent and sexual offenders register (ViSOR) and disclosure schemes

The violent and sexual offenders register (ViSOR) is a national (UK-wide) database developed to support the work of MAPPA. It can be accessed and updated by the three responsible authority agencies and contains records of individual offenders who are considered to pose a serious risk of harm to the public. Collective information in the database is confidential, while information relating to individual offenders is restricted. All Category 1 offenders, plus offenders managed at levels 2 and 3, must have a record on ViSOR. The record, and crucially the risk assessment that is contained in it, travels with the offender when they move to a new area, therefore allowing relevant agencies there to put in place strategies to manage the risk posed by the newcomer. Records in ViSOR are maintained for life: 'When a ViSOR nominal ceases to be an active MAPPA case, it will be archived. This means that the information will remain within ViSOR and, if necessary, can be re-activated. The nominal record will be retained until the 100th anniversary of the individual’s birth. At this point, it will then be reviewed and, in most cases, will be removed from ViSOR' (Ministry of Justice 2017a: 51).

The management and reduction of risk are central to the operation of MAPPA, and in some cases information regarding offenders managed through these arrangements can be shared with a third party: ‘Disclosure of the details of MAPPA offenders to a third party must comply with the law, must be necessary for public protection, and must be proportionate’ (Ministry of Justice 2017a: 57). Third party disclosure most commonly occurs with schools, colleges, employers, and current or former partners of offenders. Two disclosure schemes are in operation with MAPPA offenders: the child sex offender disclosure scheme (also known as ‘Sarah’s Law’), and the domestic violence disclosure schemes (also known as ‘Clare’s Law’). As their names suggest, both schemes were developed in response to cases where the victims were killed by individuals who had prior convictions for sexual assault and domestic violence, and who went back to offending once they had been released from prison. The schemes aim to make information that might help to prevent the victimisation of children or people at risk of domestic violence more readily available. In both cases, if the authorities decide that a disclosure can be made to a concerned individual, the information received by the third party cannot be shared with others.

As each police force maintains its own records, aggregate data for England and Wales are not available for the child sex offender disclosure scheme. A note published by the House of Commons Library summarising the initial pilot of the scheme in 2008-2009 found that ‘a total of 585 enquiries were made. Of these, 315 were proceeded with as applications, resulting in 21 disclosures being made’ (House of Commons Library 2012: 1). More recently, the scheme has been surrounded by some controversy, with data showing that ‘[f]ewer than one in ten applications to find out whether a person working with children has been a sex offender are granted by police’ (Coates, 2016), with charities voicing concerns that ‘there is a postcode lottery over whether forces disclose the information’ (ibid.). As for the domestic violence disclosure scheme, in the year ending June 2017, 8,490 applications were made across England and Wales, resulting in 3,410 disclosures (ONS, 2017).

2 Not all police forces were able to provide data, so this might be an underestimation of the actual amount.
The most recent evaluation of MAPPA was jointly published in 2015 by HM Inspectorate of Probation and HM Inspectorate of Constabulary as a follow-up to a previous inspection carried out in 2011. The 2015 report found ‘measurable improvement in the quality of work undertaken with MAPPA offenders managed at level 2 and 3 compared with 2011. However, risk management plans were still not good enough, the quality of minutes, while undoubtedly better, remained inconsistent, and Responsible Authorities and Duty to Cooperate agencies were not always appropriately represented at level 2 and 3 meetings’ (HMI Probation and HMI Constabulary 2015: 8). Unfortunately, the report did not include a detailed review of level 1 MAPPA cases, which represent the vast majority of the cases managed through it, so it is hard to draw any meaningful conclusion on the current state of MAPPA from it. However, given the territorial organisation of MAPPA, it is reasonable to assume a degree of variation in the arrangements established locally throughout the UK.

‘Since 2008-2009, when the current recording standards were established and data were therefore directly comparable, the numbers of offenders in Categories 1 and 2 have almost doubled (+170% and +180%, respectively), while Category 3 offenders have almost halved (Ministry of Justice 2017b)’
section 5: key issues to consider

Some common threads can be identified throughout the issues we have discussed and analysed thus far. Here, we bring them to light in the hope that they can provide useful pointers for discussions and debates during the conference.

5.1 discrimination

Critics of British counter-terrorism legislation argue that it is inherently discriminatory and unduly targets and criminalises BAME individuals. Some of the data that we included in our analysis do lend at least some weight to this claim. Home Office data reveal that while minorities are three time more likely than white people to be stopped and searched, the likelihood of being stopped increases seven-fold for black people. Additionally, 63% of those placed under the 14-day detention for terrorism in 2017 hail from a minority background, as do 66% of people stopped in the course of border controls.

Such figures make it hard to argue against the claim of discrimination. However, the government counters that the data should not be read in light of the ethnic breakdown of the general public, but of the terrorist population. While the argument is logically sound, solid data on the demographics of those engaged with terrorism are incredibly hard to come by. As noted above, the Supreme Court of the UK has ruled that it is unlikely that the power to stop people at borders to question them about possible involvement in terror-related activities could be used in racially discriminatory ways.

Finally, while data on Prevent were not included in the analysis (as the people passing through it are neither charged nor arrested), the latest Home Office statistical bulletin on the programme reveals that 65% of those referred had been flagged for Islamist extremism, and 10% for right wing extremism (Home Office 2017d). The Programme has been criticised on a number of fronts for what its critics argue is the over-representation, stigmatisation and targeting of Muslims, particularly young boys.

Safeguarding policies might also be vulnerable to potential accusations of discrimination. In an increasingly culturally diverse society, different cultural groups will have different ideas on how to raise children and, more generally, manage inter-generational relationships. Issues such as FGM require authorities to pull off a particularly difficult balancing act. On one hand, they have to put in place strategies to protect young girls who might be at risk of undergoing the practice. On the other, sensitive and culturally informed engagement with specific communities is essential.

Efforts have been made at raising awareness of the issue of FGM among relevant stakeholders, and since 2014 NHS hospitals are required to report whether a woman has undergone FGM. In the same year, FGM was for the first time mentioned by the then education secretary Michael Gove in his letter on safeguarding guidelines sent to schools. Along with awareness, so is the institutional response to FGM growing. As with the Serious Crime Act 2015, a protection order can now be issued to place in temporary care girls thought to be at risk of FGM, so as to examine them to assess whether or not they have undergone the practice. However, significant delays have meant that that girls can spend months separated from their families, therefore suffering unnecessary trauma. As of today, no one has been convicted for FGM offences in a UK court, and some doctors have argued to the BBC that the phenomenon is not taking place at the rate politicians suggest (Kirkland 2017).
5.2 media

The media play a fundamental role in shaping people’s view and understanding of the world, and they provide us with the frames of references through which we give meaning to events. The explosion of digital technologies and social media has radically altered the landscape. We no longer have to rely on the opinions of experts or media professionals, and instead can turn to a never ending range of internet channels, bloggers, social media personalities to form our ideas on what is happening in the world. Two troubling phenomena enabled by social media are of relevance to the issues being discussed here, and are worth analysing in greater details: vigilantism and Islamophobia.

Some crimes stick to the collective memory of a nation. The murder of James Bulger in 1993 by two ten-year olds, Jon Venables and Roberts Thompson, is one of such instance. The facts are well known, and only a brief summary will be offered here. After being released from custody, the boys were placed on life-long licences and given new identities to protect them from retaliatory attacks. A worldwide injunction to media was also issued, so that no details of their new lives could ever be made known to the public. However, a quick search on Twitter reveals that over the years several users have relied on the platform to share supposed photos and sightings of Venables and Thompson. Two men were given suspended sentences in 2014 for sharing such images via Facebook and Twitter.

Similar efforts are being made to discover the new identity granted to Maxine Carr, who in 2002 provided a fake alibi to her then boyfriend, who was later convicted of killing two 10-year old girls in Soham, Cambridgeshire. Despite the courts proving that she did not know that he had killed the girls, she has since been the victim of much hatred and has been granted the same right to anonymity as Venables and Thompson (Bowcott 2017).

Research conducted by Demos has also shown how Twitter can be used to target Muslims, with the use of anti-Islamic language spiking in the aftermath of terrorist attacks. Analysing tweets sent between March and July 2016, the authors of the report note that ‘Twitter is, in general, a real-time, reactive and event-specific platform, and most of the anti-Islamic activity identified was likewise linked to an event that had recently happened. (…) Many of the Tweets identified as derogatory and anti-Islamic included specific references to recent acts of violence and attacked entire Muslim communities in the context of terrorism’ (Miller, Smith and Dale 2016).

When the culprits in many of the CSE scandals across the country were identified, voices were raised asking if the authorities’ fear of being perceived as racist had delayed them from taking action sooner: The fact that Muslim men of British Asian heritage were abusing and trafficking white girls was seen as particularly problematic, and there is no doubt of the scale or severity of the abuse that victims had to endure. However, in another case of extensive child abuse, concerning Jimmy Savile, neither religion (Roman Catholicism) nor ethnicity (white British) were regarded as crucial elements, and media coverage did not focus on them within the context of the crimes.
5.3 privacy and proportionality

The very recent revelation of the actions of Cambridge Analytica has put Facebook under the spotlight for the way in which it manages and shares its users’ data with third parties. It remains to be seen whether the scandal will have any lasting consequence for the social media network. However, any frank conversation on how to handle one’s data, the precautions we should take to strengthen control of them, and more generally on the right to privacy in the digital age can only be very welcome.

It is now technically possible to track people’s activities, both online and offline, in ways that would have seemed impossible just a few decades ago. However, the fact that it can be done does not necessarily mean that authorities, or corporations, should do it. Privacy considerations must be balanced against other factors; in the case of terrorism, public protection is obviously paramount. Blanket collection of data that might possibly be used in the future is problematic because of how vague and indeterminate it is, but this does not mean that all surveillance of offline or online activities should be abandoned. Data protection legislation explicitly acknowledges this, and surveillance is deemed to be lawful when it is necessary and proportional. The issues then become how, as a society, we can decide what level of surveillance is necessary, what is proportional, through what mechanisms can it be carried out, and what safeguards should be put in place to prevent its abuse.

When it comes to counter-terrorism measures, it is hard to settle the question of which rights we should consider and balance, in order to address these issues. We can expect different people to come to different conclusions. While some might think it is fair for authorities to keep an eye on someone who has voiced their support or opposition to a particular policy on social media, others might disagree with them.

A convincing argument can be made that we should not police someone’s thoughts, only their actions, and that the protection of free speech should not be curtailed on a wide scale because of the risk posed by a limited number of individuals. Similarly, we should carefully consider if, and to what extent, the right to protection of the public in general, and of vulnerable people in particular, can trump an offender’s right not to be shunned and stigmatised for life.

It may also be worth asking if the public has unrealistic expectations on how offenders are punished and managed within local communities. It bears repeating how MAPPA manages offenders who have served their sentence and, as such, have paid their debt to society. Therefore, questions can and should be asked concerning the fairness of these arrangements for people with criminal records, and the extent to which we should sacrifice an individual’s right to a private life and their possibility of fully reintegrating into society, within the context of growing calls for public protection. As detailed above, records in ViSOR are maintained for 100 years. At the same time, we know that the aggregate offending behaviour peaks in mid to late adolescence and then decreases in adulthood. We are also well aware of the enormous difficulties in finding suitable accommodation and employment that people with criminal records face upon release. In light of this, it may be time to question whether we should continue to further penalise offenders by disclosing convictions, in order to prevent harm to the public, and to ask ourselves what our approach to risk says about attitudes towards guilt, punishment and forgiveness in our society.

‘A convincing argument can be made that we should not police someone’s thoughts, only their actions, and that the protection of free speech should not be curtailed on a wide scale because of the risk posed by a limited number of individuals.’
section 6: conclusion

This briefing has provided an outline of some of the key issues that should feature in any discussion of the relationship between the state and citizens, and the duties of one party to the other. It has touched upon police powers, surveillance legislation, safeguarding policies, and risk management practices to help delegates at the forthcoming Cumberland Lodge police conference to navigate the complex terrain of public protection, what authorities are doing to keep us safe, and from what risks and with what consequences.

These are vexing issues that can provoke strong and conflicting feelings and opinions. Central to these discussions are the fundamental issues concerning how a democratic society should function and the role the police can and should play in protecting citizens from harm, balanced against safeguarding the fundamental human rights of all its citizens. We hope that this conference will provide a forum where these issues can be addressed openly and in an informed way, and that this briefing document will assist the facilitation of this process.

‘Central to these discussions are the fundamental issues concerning how a democratic society should function and the role the police can and should play in protecting citizens from harm, balanced against safeguarding the fundamental human rights of all its citizens’

Coates, S. (2016), 'Sex offender data is not being shared', The Times, 11 October 2016, available at: https://www.thetimes.co.uk/article/sex-offender-data-is-not-being-shared-t9x66sjkj


