# SECURITY THROUGH HUMAN RIGHTS

Dr. Israel Butler

# *Table of contents*

# Note to readers

This background paper is a tool for non-governmental organisations (NGOs) working to counter the rollback of human rights standards taking place in the name of counter-terrorism. The document presents an alternative narrative, according to which security can only be protected if human rights standards are properly implemented. It analyses two rights-violating counter-terrorism measures (mass surveillance and ethnic profiling) and explains that these tools are ineffective and counter-productive. In contrast, alternative counter-terrorism policies that are rights-compliant are effective to deliver public safety. Although the paper concentrates on two counter-terrorism tools, the general argument that human rights make societies safer can probably be applied to other rights-violating counter-terrorism measures. The paper provides NGOs with the strongest arguments and evidence available to help them advocate in favour of human rights standards. All arguments have been substantiated with reference to reliable (and, where appropriate, academic) sources so that readers can follow up and adapt those points most pertinent for their own advocacy.

This paper does not necessarily reflect the opinions of the members of the Civil Liberties Union for Europe.

The author would like to thank Natalija Bitiukova, Jelle Klaas, Eefje de Kroon, Doutje Lettinga, Cristina de la Serna Sandoval, and Lydia Vicente for their feedback and comments on an earlier draft. All errors remain my own.

# *Executive summary*

### Governments pit security and human rights against each other

Terrorist attacks in Europe have placed political leaders under intense pressure to take measures to make the public feel safe. Governments have reacted by expanding the powers of security services, including by authorising mass surveillance and lowering the threshold of proof required by security services to stop and search individuals or their property. In several countries, stop and search powers have been used mostly against (people perceived to be) Muslims, which amounts to ethnic profiling. Although these measures violate human rights law, governments argue that human rights obstruct the work of security services and should be subordinated to the goal of security, because without security no one can enjoy their human rights. The public appears to have generally accepted or acquiesced to this narrative.

> *"mass surveillance has never helped to identify a terrorist suspect or prevent a terrorist attack in the West"*

### Human rights advocates can win back public opinion

Human rights organisations have had difficulty persuading the public to reject these unjustified limitations on their rights. To turn public opinion, rights groups should alter their advocacy in three ways. First, the rights movement needs a single overarching narrative that can be advanced consistently by all those who advocate against the rollback of human rights in the name of security. To date, organisations in different human rights sectors (such as media freedom, racial equality, digital rights, fair trial rights, the freedoms of NGOs) have advanced messages particular to their field of work. This has led to the public receiving numerous disconnected pro-human rights messages, which weakens the power of advocacy. Second, rights advocates need to show that mass surveillance and ethnic profiling are ineffective to combat terrorism and actually threaten security. Third, rights advocates should increase the value attached to privacy in public opinion. Advocates working on privacy have generally reaffirmed a narrow understanding of the concept as a personal right to hide secrets. In the public mind, sacrificing personal secrecy is an acceptable price for the security they believe is delivered by mass surveillance. Rather, privacy advocates should develop a broader concept of privacy and explain its collective benefits for democracy.

## Mass surveillance is useless to prevent terrorism and jeopardises public safety

The authorities argue that mass surveillance provides vital intelligence to identify terrorist suspects and prevent attacks. Research into the contribution of mass surveillance programmes in the USA finds that mass surveillance has never helped to identify a terrorist suspect or prevent a terrorist attack in the West.

Neither is mass surveillance (including data retention) necessary for investigating crimes after they have been committed. This is because the information that is usually of interest to security services has long been collected by internet and phone companies as part of their normal business, including the location from which calls are made or numbers dialled.

Mass surveillance requires financial and staff resources to store, filter and analyse the information collected, and to follow up on potential suspects flagged by this system. This means that resources are being wasted on a policy that does not improve security.

In contrast, putting resources into more traditional targeted surveillance would have a big impact on public safety. In the vast majority of terrorist attacks in Europe since 9/11, some or all of the perpetrators were known to the security services. Security services failed to act in time for a variety of reasons. In some cases, resource constraints meant that they had to abandon targeted surveillance of a suspect to deal with other priorities.  In other cases security services failed to communicate internally or failed to act on information supplied by other governments. Mass surveillance has become a lethal distraction and waste of resources that is making it more difficult for security services to use effective methods of gathering intelligence that guarantee security.

## A broader concept of privacy: mass surveillance is destroying democracy

As well as endangering our security, mass surveillance is also undermining democracy. A large body of research from the disciplines of social psychology and communications studies proves that when human beings are in public or feel they are being watched, we are reluctant to express ideas and opinions that differ from majority held opinions or social rules. Recent studies and surveys also show that because the public is now aware that governments use mass surveillance, people tend to view phone and internet communications as a public space where they have no privacy.

It seems that this tendency to conform to the majority-held opinion and social rules is hardwired in humans. Historically, disagreement with the majority may have led to expulsion from the group or denial of resources resulting in hardship or death. In experiments, when an individual disagreed with the group this led to reactions in parts of the brain associated with pain, while expressing agreement with the group triggered the production of oxytocin, also known as the ‘love’ hormone.

Without privacy, individuals are unable to develop and spread ideas that might challenge majority opinions and existing rules. There are broadly two categories of people responsible for the creation and spread of ideas. First, opinion-shapers, who are so confident in their ideas that they are not put off by hostile or sceptical majorities. Second, the rest of the public, who are either convinced of, or go along with, majority opinions and rules.

*“In the vast majority of terrorist attacks in Europe since 9/11, some or all of the perpetrators were known to the security services”*

Those who shape public opinion (such as journalists, philosophers, politicians, academics, or activists) require privacy to research, create and test ideas or new information. Concepts that are now widely accepted, such as racial or gender equality, universal suffrage, the sharing economy or environmentalism were once considered outrageous by majority opinion. Unless opinion-shapers can evaluate and refine their ideas in private, they will not be confident enough to promote them in public. In turn, members of the general public require privacy to research and evaluate these ideas and pieces of information and decide whether they agree. Without privacy, the pressure to conform to existing opinions and rules is so heavy that individuals are reluctant to admit to entertaining potentially controversial ideas.

Mass surveillance makes it much easier for the authorities to monitor opinion-shapers. As a result, opinion-shapers are more reluctant to carry out their work because they feel that they are more likely to be sanctioned in some way, such as losing one’s job, being harassed, having one’s property searched or losing funding. It is well documented that the authorities have used these tactics against politicians, activists, NGOs, academics and journalists working on issues including racial equality, human rights, social justice, the anti-war and anti-nuclear and environmentalist movements.

Because a substantial proportion of the public now views communication over phone or internet as being in the public sphere, individuals are self-censoring their opinions and refraining from using these technologies to communicate or carry out research. In turn, this means that they are unable to make informed decisions over whether to accept or reject current opinions and rules or whether to approve or not of their political leaders and their policies.

Because mass surveillance makes it harder for new opinions and rules to emerge, our societies will find it difficult to adapt to new challenges, hold our leaders accountable or make good quality decisions.

### Ethnic profiling is ineffective and endangers public safety

Examples of ethnic profiling in the sphere of counter-terrorism can be found in Germany (the ‘rasterfahndung’), the USA (special registration, travel bans targeting certain Muslim-majority countries) and, more recently, France (in particular, property raids). There is little evidence that these operations uncovered terrorist activity. Ethnic profiling is inefficient and increases the threat to security, for two reasons. First, it creates a blind spot that is exploited by terrorist groups who simply deploy individuals that do not belong to the suspect minority group. Individuals involved in violent extremism belong to a wide variety of nationalities and ethnicities, including an increasing number of white Western converts. Second, ethnic profiling makes minorities distrusting and suspicious of security services, which makes them less likely to cooperate with the authorities and contributes to marginalisation, which makes individuals more vulnerable to radicalisation.

### Intelligence-gathering measures that respect human rights are most effective

Instead of investing in mass surveillance governments should focus on effective methods of collecting intelligence that comply with human rights law. First, governments should give security services more resources to carry out targeted surveillance, while incorporating judicial and parliamentary oversight to prevent abuse.

Second, governments should invest in the most common source of intelligence: the public. Community-oriented policing based on a genuine respectful partnership can create trust and personal relationships between law enforcement personnel and the community they serve. This in turn creates an environment where the public spontaneously offers intelligence to local police.

Third, security services should abandon ethnic profiling in favour of behavioural profiling, according to which individuals are targeted only on the basis of objective evidence, such as suspicious behaviour. In cases where security services have replaced ethnic profiling with behavioural profiling the overall number of individuals stopped by police falls, the number of suspects caught in searches rises, and the proportion of ethnic minorities stopped, falls.

### Governments can reduce radicalisation by implementing their human rights obligations

Research shows that it is not possible to draw up a profile of a typical violent extremist or to predict who will resort to terrorism. However, there is agreement around which factors make people more vulnerable to radicalisation.

First, the existence of intense anger or frustration caused by an actual or perceived injustice. This can come from an experience of discrimination, marginalisation or exclusion - either personal or vicariously on behalf of one’s ethnic or religious group. These feelings can also arise from perceived injustices committed against one's group in other parts of the world, such as the West's involvement in armed conflict or collaboration with repressive regimes in the Middle East. Second, the absence of a strong sense of identity or sense of purpose, which may arise because of inconsistencies between or dissociations from national, cultural or religious identities or lack of education or employment. Third, these factors create a 'cognitive opening' where the individual wishes to correct these injustices and starts looking for answers to explain why the world as they see it is so unfair and how they might change it. This opening is filled by extremist ideology that twists religious teachings and provides a ready-made narrative maintaining that an evil, morally bankrupt West is repressing and humiliating Muslims worldwide. Fourth, the process through which this narrative is adopted by an individual, and through which the moral taboos associated with killing innocents break down, generally takes place in a group or network where its members radicalise each other often under the supervision of a mentor.

European governments trying to prevent radicalisation focus on the final stages of the process and try to stop individuals from being convinced of the answers given by extremist ideology. It is difficult to identify potential suspects and to do so the authorities have to monitor entire communities. This fuels feelings of suspicion and marginalisation among minorities, which increases their vulnerability to radicalisation and distrust towards the authorities.

Instead, governments should address the underlying factors that create the 'cognitive opening' in the first place. This would significantly curtail the flow of individuals into violent extremism. The authorities can achieve this by implementing their human rights obligations, both domestically (to promote equal access to education, employment, health care and non segregated housing) and during the course of their international relations.

*"Without privacy, individuals are unable to develop and spread ideas that might challenge majority opinions and existing rules"*

**The over-arching message: human rights keep us safe**

If governments were to implement their human rights obligations, Europe would be safer from terrorism. Mass surveillance and ethnic profiling are useless to fight terrorism and make us less safe. Many attacks could have been prevented if security services had been given adequate resources to continue targeted surveillance of suspects or were more efficient at sharing and acting on information. Governments should properly resource law enforcement agencies to carry out targeted surveillance (with appropriate safeguards), invest in community-oriented policing and abandon ethnic profiling in favour of behavioural profiling. Combining these measures with policies to promote equality and inclusion for minorities and an ethical foreign policy would deliver long-term security. By implementing their human rights obligations, governments will minimise threats to security, and allow threats that do emerge to be dealt with more effectively. Put otherwise, human rights keep us safe.

# Introduction

In the name of fighting violent extremism, European governments have progressively introduced a number of measures that violate human rights law. Broadly speaking, the authorities have argued along the following lines: terrorists want to destroy 'Western' values, including human rights; we must not let terrorists win by compromising these values, but we cannot ensure the survival of said values without guaranteeing our security; we cannot guarantee security without sacrificing our human rights, because human rights make it more difficult for security services to perform.[2] This rhetoric, which the human rights movement has had difficulty countering, has won over significant public support.[3]

It has been suggested that human rights organisations have had difficulty winning the rights versus security debate because different sectors – with their own specialisations – have each formulated their own counter-arguments.[4] Non-governmental Organisations (NGOs) working on equality have concentrated on the problem of ethnic profiling; civil liberties NGOs have focussed on the right to privacy, due process and on abuse of suspects by security services; digital rights NGOs have focussed on how individuals are losing control over their data, which can be misused by companies and the authorities to build (erroneous) profiles that damage the lives of individuals and social groups; free speech NGOs have focussed on the impact on journalism and democracy; others have focussed on questioning the effectiveness of counter-terrorism measures. This has meant that the public has heard a variety of arguments in defence of various aspects of human rights but has not heard a single, unifying, clear and consistent message from NGOs.[5]

This paper proposes an alternative narrative: to guarantee security, governments must implement human rights standards. Discussion will concentrate on two rights-violating measures that are being deployed in the name of security: mass surveillance and ethnic profiling. These measures undermine public safety. Mass surveillance is ineffective to prevent terrorist attacks or identify terrorists. It also constitutes a drain on the limited resources of security services and distracts law enforcement agencies from focusing on existing intelligence that would prevent attacks. Ethnic profiling creates mistrust and suspicion between security services and ethnic minorities, which makes these groups less likely to cooperate with and volunteer intelligence to security services. Ethnic profiling also distracts security services by focusing their attention on minorities matching erroneous profiles, making it easier for genuine suspects to avoid detection. Beyond counter-terrorism policy, failures by governments to implement their human rights obligations in the context of foreign and social policy contribute to public insecurity. In particular, subordinating rights promotion to economic and other political goals in foreign relations while failing to promote racial equality at home increases the vulnerability of segments of society to radicalisation and violent extremism leading to terrorism.

If governments wish to keep the public safe, then security services should implement methods of gathering intelligence that are proven to be effective; namely, targeted surveillance under judicial scrutiny, behavioural profiling and community-oriented policing. Governments should also implement their legal obligations to promote racial equality for marginalised ethnic minorities and prioritise respect and promotion of human rights among the goals of foreign policy.

This is not to say that human rights tools should be co-opted into counter-terrorism strategies. Rather, it is to say that implementing human rights standards is an effective, holistic and sustainable means of delivering security.[6] The alternative narrative proposed here does not pretend to be entirely original – it draws together many of the existing arguments advanced by NGOs working in different sectors. Its contribution is rather, first, to weave these arguments together into a single coherent and short message; and second, to flesh out some of the missing connections between the arguments, such as the link between privacy and democracy, or ethnic profiling and intelligence-gathering.

Some rights advocates may prefer to oppose mass surveillance and ethnic profiling on principle alone, rather than arguing that these measures are ineffective and counter-productive. This position is based partly on concern that effectiveness-based arguments weaken the pro-rights position, because if evidence showed that these measures could be made effective, then rights advocates would have nothing to fall back on. However, the two positions can be reconciled. Legally, when the state implements a measure that interferes with a right, this must be proven to be necessary and proportionate. That is, the proposed interference must be effective – it must be apt to achieve the intended legitimate aim.[7] Furthermore, even if particular measures that interfere with a right might be proven to be effective, if they destroy the essence of a right, they will not be legally permissible.[8] Put otherwise, effectiveness arguments do not undermine rights-based arguments. If anything, they go hand in hand.

Part I will focus on mass surveillance, examining its contribution to security and its impact on privacy and democracy. Part I will also examine the privacy versus surveillance debate, propose an alternative concept of privacy and explain the link between privacy and democracy, which has been inadequately explained by privacy advocates. Part II will discuss the contribution of ethnic profiling to criminal law enforcement and counter-terrorism. Part III will propose alternative counter-terrorism measures that have a proven record of effectiveness in delivering security, and which can be made compatible with human rights standards.

# Part I: Mass surveillance [9]

The USA and many European countries routinely carry out mass surveillance of their own and foreign populations. In many cases, this has been done in secret, without legal authorisation (namely, judicial or parliamentary oversight), or using vague or out-dated legal provisions that did not explicitly authorise mass surveillance.[10]

### I.A: Why mass surveillance is ineffective in practice

**[Targeted surveillance, mass surveillance, metadata, content data]**

*When security services identify a suspect, they may decide to watch and follow this individual and read and listen to their calls, emails and conversations to collect evidence of a crime. Watching a specific suspect is known as targeted surveillance, and is a well-established technique used to investigate and prevent crime. To prevent the police abusing their powers and investigating individuals who are not suspected of doing something illegal, international standards require security services to get the permission of a judge or similar independent authority before they can place a suspect under surveillance.*[11]

*In contrast, mass surveillance – also known as 'bulk' or untargeted surveillance – is not aimed at a specific suspect. Mass surveillance involves the interception of large quantities of information sent over phone or internet services – for example, all the phone records and internet histories or all text messages and emails sent by everyone in a given country. This information is kept for a number of months or years so that security services can search through it. Security services search the information using certain criteria to try to identify people involved with terrorism and crime. For example, they may search for messages that include certain words (e.g. 'caliphate' or 'bomb') or calls made to or from a particular country (e.g. Afghanistan or Iraq) to a particular city (e.g. Brussels). Mass surveillance is supposed to allow security services to look for new threats that they do not already know about.*[12]

*The information collected through untargeted or mass surveillance can be broadly divided into two categories. First, metadata (also known as 'communications data'), which identifies things like the websites a person visits, credit card transactions, the email addresses of persons an individual writes to, the subject lines of emails, the phone numbers a person calls and to which he/she sends text messages, their posts to social media as well as their location.*[13] *Second, content data, which refers to the actual content of an email, text message, phone call, or video call (e.g. over Skype or Facetime).*

In an attempt to calm public concern over mass surveillance, the authorities frequently argue that people should not be worried about security services collecting their metadata because this does not allow the authorities to listen to or read the contents of a conversation. However, metadata paints a very clear picture of who we are and what we do and think, and it is much quicker to find these things out from our metadata than it is to read through our emails.[14] The websites a person visits for news, entertainment or research and their online purchases give an indication of their political or religious views, hobbies, personal interests and lifestyle. Even if one does not read their content, emails sent to or from a lawyer, doctor, psychologist or bank show a person may have health, family, financial or legal problems. By looking at how often someone sends and receives messages from a particular number or email address, a person can work out the identity of your friends and how emotionally close you are to them and your relatives. The subject lines of someone's emails show what issues that person is speaking about.[15] Location data (routinely collected by applications on smart phones) shows a person's daily habits – where he/she lives and works, which shops he/she visits, his/her favourite bars and cafes, what time he/she tends to go to the gym, where he/she is when a photo is taken, a message is sent, or a post is made through social media (such as LinkedIn, Twitter, Pinterest or Facebook).[16]

Until recently, EU law (the Data Retention Directive) required communications service providers (like the companies that provide mobile phone or internet services)[17] to collect metadata.[18] In 2014, the EU's Court of Justice declared that this legislation was illegal because of how seriously it invaded individuals' privacy.[19] In 2016, the EU's Court of Justice also found that national legislation that some governments introduced to replace the Data Retention Directive was also illegal.[20] Despite this ruling, most countries in the EU still collect metadata.[21] Some EU countries, such as France, the UK, the Netherlands, Hungary, Lithuania and Poland, have recently created, or are in the process of creating, new laws that would give security services the power to collect content data or metadata.[22]

Once metadata and content data have been collected from the internet, security services then try to narrow down the amount of data that they will search and analyse. They do this by searching the data using certain criteria. Data that matches these criteria is kept for further analysis, and data that does not match is put to one side. These search criteria might be certain key words appearing in emails or messages, the locations from which messages were sent or received or other patterns of communication. Even though filtering the data collected in this way helps to reduce the amount of information that analysts have to examine, the volume of data that matches the criteria is still extremely large – still too much for security services to analyse. For example, recently leaked documents reveal that UK intelligence services collect far more information than they are able to analyse or use – figures for one UK surveillance programme showed that 97% of the data collected was not even being read.[23]

When security services do try to analyse the data, it requires considerable resources. This is because even after the data is filtered to keep only the information that matches the search criteria, most of the individuals identified will be innocent (referred to as 'false positives').

Furthermore, the search criteria will also miss some potential suspects (referred to as a 'false negative').

In reality, the situation would be significantly worse. The sources cited above point out that it is impossible that the security services could hope to develop such accurate searches, partly because terrorists constantly adapt their methods to avoid detection, such as changing how they communicate, the software they use or the code words they use. So the number of innocent people identified as terrorists, and the number of terrorists who are not identified at all, would be much higher. This illustration of how mass surveillance works helps to explain why, in practice, this tool has never been useful to identify a terrorist suspect or prevent an attack (discussed below).

## *Wild goose chase*

Statisticians have tried to illustrate the ineffectiveness of mass surveillance using a hypothetical example. They present an imaginary scenario according to which the security services have developed a method of detecting a terrorist according to their voice.[24] This machinery is assumed to be 99% accurate. That is, when anyone makes a phone call, this machine will automatically detect with 99% accuracy whether the individual in question is a terrorist. Let us imagine that the security services use this equipment in a country with a population of 60 million people, where they estimate that 3,000 people are involved with terrorism.[25] A 99% accurate detection method would correctly identity 2,970 of the 3,000 terrorists. Thirty terrorists would not have been identified at all and would escape the attention of the security services. Furthermore, because the system is only 99% accurate, it would also identify 1% of the general population as terrorists. That would amount to 600,000 innocent people wrongly identified as terrorists.

The security services then have to carry out further investigations to be able to find the 2,970 genuine suspects from among the 600,000 or so people identified by the system as terrorists. Journalists in the USA report that something similar occurred after the 9/11 attacks. Hundreds of FBI agents were sent to investigate thousands of potential suspects flagged by the NSA's mass surveillance programmes as potential suspects. These investigations invariably led to dead ends and diverted officers away from carrying out investigations built on more traditional and effective methods.[26]

### *I.B: The mass surveillance debate: 'nothing to hide'* [27]

Governments argue that mass surveillance is necessary to prevent terrorism and serious crime. The main objection to mass surveillance from the public and from activists is that it violates privacy.

> **[Nothing to hide]**
>
> *Advocates of mass surveillance argue that individuals who have 'nothing to hide have nothing to fear' from the authorities. They maintain that security services are only watching out for criminal activity and are not interested in intimate, personal or confidential information. The 'nothing to hide' argument frames privacy narrowly, in two ways. First, it portrays privacy as being of value only to the individual. Second, it portrays privacy as something negative, which is used to conceal discreditable secrets. Defenders of privacy have countered with a 'right to hide' argument. However, this has only reinforced a narrow understanding of privacy, which does not appear to be important enough to outweigh the desire for security that the public believes can be delivered by mass surveillance.*

#### *I.B.i: The individual dimension of privacy*

Privacy is important to us as individuals for at least two purposes.[28] First, humans tend to choose to be alone or with close friends or relatives so that we can take a rest from fulfilling a particular role (parent, colleague, sibling, boss), unwind, express intimacy or recover from a difficult experience like a rejection. Second, for certain activities, we tend to want a degree of anonymity, whether in the physical world or online.[29] This can include when we want to test out new experiences, do something that breaks social convention, or when we need to address personal problems with a professional like a doctor, lawyer or psychologist.

The 'nothing to hide' argument does not necessarily contend that privacy is not important to individuals. Rather, it maintains that the security services do not really threaten individual privacy: even though the authorities collect everyone's information, they have no interest in our personal lives and will only examine data to prevent or solve crimes. Governments also maintain that even if the simple act of collecting information interferes with privacy, this minimal intrusion is justified to protect national security. In a nutshell, the state argues that it does not really invade our privacy, and even if it does, this is a small price to pay for safety.

#### *I.B.ii: Privacy as secrecy*

The second element of the 'nothing to hide' argument undermines the legitimacy of privacy by labelling it a vice. The authorities are implicitly saying that our information can only fall into one of two categories: personal information, or information about illegal activities. According to the government narrative, the public has no reason to object to mass surveillance on privacy grounds because our personal information is safe. Because, according to our governments, security services are only interested in information about crime, anyone who insists on opposing mass surveillance must be doing so not because they care about their privacy, but because they are hiding illegal behaviour.

Put otherwise, the authorities' position is that privacy's only value is to preserve secrets: either secrets that the security services are not interested in, because they are personal, or secrets that the security services are interested in, because they are illegal. Public safety is more valuable than personal secrets, which the security services are not interested in anyway. And illegal secrets do not deserve secrecy.

### *I.B.iii: 'Right to hide'*

Privacy advocates have confronted the 'nothing to hide' position with at least three 'right to hide' arguments.[30] The first concerns the psychological impact of mass surveillance. There is some evidence to suggest that a lack of personal privacy can lead to mental health problems.[31] However, this is probably a weak argument for advocates fighting against mass surveillance. This is because most of the empirical evidence concerning the impact of surveillance on mental health is taken from studies of surveillance in specific institutional settings with a clear relationship of hierarchy, such as surveillance in the workplace, schools and prisons. This is probably not very convincing for the public because it is not easily comparable to more subtle mass surveillance by the security services. In the absence of more directly pertinent evidence, the assertion that mass surveillance is leading to stress, anxiety, depression and violence among the general population is unlikely to sway the public.[32]

A second foundation for the 'right to hide' argument is based on the safety of information once it has been collected and placed in databases. There is evidence that security services have abused their powers by monitoring perfectly legal activity, for example by stalking love interests and viewing and sharing compromising photos and videos of members of the public.[33] As will be discussed below, data can also be stolen by criminals, foreign governments and terrorists who may misuse it in multiple ways – including for blackmail, theft and murder. The more examples that can be found and publicised, the more the public may see that mass surveillance poses unacceptable risks. This is a potentially powerful argument. However, it may be more likely to convince the public that they require better safeguards to ensure appropriate data protection rather than prompting people to call for an end to mass surveillance altogether.

The third 'right to hide' argument questions the way that the 'nothing to hide' camp categorises behaviour in a binary manner as either personal or illegal. This position argues that there is a third category: legal behaviour that goes against social conventions or majority views. According to advocates, concealment does not imply illegality. Concealment merely allows individuals to escape being judged (embarrassed or shamed) for unconventional but lawful behaviour.

This is an inherently hard argument to win, because even if it denies illegal behaviour, proponents of this argument are necessarily 'outing' themselves as hypocrites who engage in socially unconventional behaviour that they wish to conceal from other people.[34] As will be discussed below, individuals tend to be reluctant to admit openly, outside the safety of a trusted audience, to diverging from social norms. This will make it difficult to motivate significant proportions of the public to support a 'right to hide' couched in these terms.[35]

#### *I.B.iv: Reinforcing privacy as secrecy for the individual*

The broader problem with all 'right to hide' arguments is that they reinforce a narrow understanding of privacy as a right whose only purpose is to allow individuals to keep secrets. When presented with a choice between preserving personal secrecy or guaranteeing security, a large proportion of the public has chosen security, which they believe can be delivered by mass surveillance.[36] If campaigners wish to tip the scales in favour of privacy, they should attack both sides of the equation. First, promote a broader understanding of privacy that focuses more on its collective benefits to social innovation and democratic accountability. Second, consolidate the currently scattered evidence that proves that mass surveillance is failing to deliver on its promise of security.

### ***I.C: Broadening the arguments against mass surveillance***

The remainder of Part I of this paper will argue that mass surveillance is both ineffective against terrorism and a threat to security. It will then propose a concept of privacy that goes beyond concealment: the liberty to think, form opinions and make decisions freely. This understanding of privacy helps to explain the collective functions of this value, in particular its role in democracy (both social innovation and democratic accountability). The remainder of Part I will then explain how mass surveillance interferes with the collective dimensions of privacy.[37]

#### *I.C.i: Testing the arguments about mass surveillance and security*

The following section sets out the case that mass surveillance is not a necessary (or even a useful) tool in the fight against terrorism and crime. Contrary to what we are told, mass surveillance does not make us more secure, but rather makes us more vulnerable to terrorism and crime.

##### *I.C.i.a: Mass surveillance has never helped to prevent terrorism*

Mass surveillance has never been useful to prevent a terrorist attack, or even to identify a terrorist suspect.[38] This is the conclusion reached by two pieces of research into the NSA's mass surveillance programmes. One report was produced by a US think tank and based on an analysis of over 200 cases concerning individuals indicted, convicted or killed abroad because of their involvement in an act of terrorism since 2001. The other was produced by a US congressional oversight committee, based on interviews with security service staff and access to classified documents, among other sources. The research finds that even where information discovered through mass surveillance has revealed evidence connected to terrorist activities, the same information was already available to security services through traditional forms of investigation, such as targeted surveillance, informants or tip-offs from the public. Put otherwise, the available evidence shows that mass surveillance has been useless to prevent attacks in the West, or to identify terrorists.[39]

*I.C.i.b: Mass surveillance is not even helpful to solve crimes after they have been committed*

As well as failing to prevent terrorism, evidence from EU countries suggests that mass surveillance is not even useful to help resolve crimes that have already been committed. Studies on Denmark, Germany and the Netherlands investigating whether the collection of metadata under the EU Data Retention Directive has been useful to help solve and prosecute crime have found that the collection of metadata has had virtually no effect.[40] In some cases, the use of metadata made no difference to whether a defendant was convicted. In other cases, the evidence contained in the metadata that was useful to the authorities was information that telecommunications companies already collected for billing purposes before the retention of metadata was made mandatory. For example, the list of numbers to which calls are made or messages sent, what time these were made and their duration.

Some EU governments have provided anecdotal examples of when metadata has been useful to investigate criminal activity, or when the absence of metadata has been a barrier to investigations. It is difficult to identify examples where the information referred to could not been obtained through other methods, such as phone numbers kept for billing purposes, information that could be acquired through targeted surveillance during an investigation, or location data, which can be acquired by triangulating phone signals from mobile phone towers.[41]

*I.C.i.c: Mass surveillance makes us less safe by draining resources from more effective ways of collecting intelligence*

Because mass surveillance is ineffective to prevent terrorism, and is not even useful to solve crimes already committed, it means that the resources spent to collect and analyse information, and to follow up on false leads, are being wasted. This is not just an irresponsible use of taxpayers' money. It is endangering public safety.

Security services have limited resources – they must prioritise how to use their staff and budgets.[42] Research into major terrorist attacks in Europe since 9/11 shows that the security services usually already knew of some or all of the attackers involved. These include the attackers involved in the Madrid train bombings in 2004, the London bombings in 2005, and the more recent attack against *Charlie Hebdo* magazine and the Paris shootings in 2015, as well as the Brussels bombings in 2016 and the Manchester bombing and London Bridge attack in 2017. In some cases, security services decided not to monitor these individuals more closely because their limited resources required them to prioritise between targets and they chose to monitor other suspects. In other cases, security services ignored information, or failed to share information with each other, or were too slow to act on the information they were given.[43]

It seems that the only attacks where perpetrators are less likely to be known to the intelligence services as potential terrorists are those committed by 'lone actors', in particular when they are self-radicalised.[44] However, it seems that such attackers were either already known to the police for their criminal activity, and/or to other state bodies because of their mental health problems. Indeed, Europol has suggested that mental health problems may have been the main factor behind recent lone actor attacks.[45] Given that these individuals are already in contact with the authorities, it seems untenable to suggest that indiscriminate mass surveillance of the public at large would be helpful to identify them.

Mass surveillance is making the public less safe because it pulls resources away from effective counter-terrorism tools, like targeted surveillance and improved intelligence sharing, which could have helped prevent many attacks. Human resources are being diverted away from monitoring existing suspects and into analysing new information thrown up by mass surveillance. Former FBI and NSA staff have criticised this approach, explaining that security services are already trying to find a needle in a haystack when using traditional methods of intelligence gathering; collecting more (useless) data through mass surveillance just adds more hay to the pile.[46] Furthermore, governments are investing in mass surveillance instead of focusing on boosting the capacity of security services to carry out targeted surveillance. For example, in the UK, the cost of collecting the public's metadata has been estimated at around 1 billion GBP over a ten-year period, which some have argued could instead be spent on hiring at least a further 3,000 police officers (over the same ten-year period) – which would be a significant boost to staff numbers, considering that MI5 is reported to employ only 4,000 staff.[47]

### *I.C.i.d: Mass surveillance can help criminals, foreign spies and terrorists*

Electronically stored information is vulnerable. Hackers, often using tools stolen from intelligence agencies, are able to bypass security measures put in place by companies, public authorities and governments to keep personal data and commercial and state secrets safe.[48] Personal data held by private companies is frequently lost, stolen or held to ransom.[49] For example, in 2015 at least two telecommunications providers were victims of hackers who stole personal details of millions of customers and, in one case, the bank details of over 15,000 customers.[50] In 2015, a website facilitating extramarital affairs was hacked, revealing the names, addresses, phone numbers and sometimes bank details of over 30 million people (including government and military personnel), exposing them to blackmail and theft, and leading some individuals to commit suicide.[51] In 2014, hackers stole data from 500 million Yahoo accounts.[52] In 2012, data relating to the accounts of over 100 million LinkedIn members, including passwords, was stolen and put up for sale by hackers.[53] Hacking is not the preserve of cyber criminals. Facebook has warned of foreign governments attempting to hack into individuals' social media accounts, and Western security services have warned university researchers that foreign governments may attempt to steal their work through cyber espionage.[54] Russian hackers recently placed emails from the Democratic National Committee in the USA online, directly interfering in national elections.[55] Government institutions, even in countries with sophisticated security services, are also frequently victims of data theft. In 2015, a US federal government website was hacked, revealing the details of over 22 million current and former federal employees and applicants for federal government jobs, including those in sensitive positions with security services like the FBI.[56] In 2016, the Federal Reserve Bank of New York lost to hackers over 100 million USD belonging to the Bangladesh central bank.[57] Research from the UK suggests that from 2011 to 2014, there were around 400 instances where local authorities either lost or had data stolen from them. Almost 200 physical storage devices, like mobile phones and laptops, were lost or stolen during the same period. In 2014, there were over 100 instances of data loss or theft in the UK's health service.[58]

Ending mass surveillance will not necessarily prevent future hacks and thefts of data. However, mass surveillance places even more information about people into databases held by governments and private companies. The more information that is held about us in digital form, the more likely criminals or terrorists are to find a database with vulnerabilities. This increases the opportunities for wrongdoers to blackmail or steal from a target, or study a target's habits and movements in preparation for an attack.[59]

### *I.C.ii: Mass surveillance: privacy and democracy*

The previous section explained that in practice mass surveillance fails to make us safer. It is a waste of public resources and it leaves us more vulnerable to criminals, foreign spies and terrorists. Apart from undermining security, mass surveillance is also a threat to privacy. As discussed above, when campaigning against mass surveillance, rights NGOs have predominantly portrayed privacy as a right that benefits individuals. That is, most campaigners have not invested a lot of effort in explaining to the public that privacy also has collective benefits for society as a whole, in particular the role of privacy in democracy.

Some rights advocates have argued that mass surveillance is bad for freedom of expression and freedom of information, which are pre-requisites for a properly functioning democracy.[60] However, there have been few attempts by campaigners to explain how privacy plays an essential role in the free development and exchange of ideas and information that allows societies to create new rules and evaluate how existing rules are being applied by their leaders. Instead, it is more common for campaigners to draw emotive parallels between mass surveillance and George Orwell's Big Brother, while sometimes pointing out that surveillance is a tool used by totalitarian regimes to control their populations.[61]

Evidence from surveys suggests that people tend to view privacy as a personal commodity that allows them to conceal information about themselves, which they are willing to trade in return for security and even in return for commercial services, like discounted prices, free use of social networking platforms or free use of software.[62] This may be because the public is unaware of the collective (as opposed to individual) benefits of privacy, or because the link between the individual and collective benefits has not been explained convincingly. If the public can be persuaded that privacy is an inalienable and common good, rather than a tradable personal commodity, then they might become more motivated to defend it against mass surveillance. The following sub-sections offer an alternative, broader conception of privacy and explain its democratic functions.

### *I.C.ii.a: Privacy: freedom to form opinions, think and make decisions without interference*

Privacy is neither particular to Western culture nor to modern times. Anthropological studies suggest that privacy has been protected by all cultures. Societies may differ in the ways that they protect privacy and may draw the line between what is public and what is private in different places, but privacy is a universal value.[63]

Privacy is our right to choose and control what things we share about ourselves with other people. We share information, ideas, opinions, property, personal space and our bodies. We share these things with our partner, family members, friends, classmates, colleagues, acquaintances, strangers and the general public. And while we choose to share different things with different people, we also choose not to share certain things with anyone. When we have control over these choices, we can be said to have privacy.[64] When our control over these choices is taken away from us, our privacy is invaded. Mass surveillance eliminates privacy almost entirely because it results in everything we do with our phones, computers and the internet being recorded. We use these devices constantly for almost all aspects of our lives. As a result, we have lost control over how we share information about ourselves.[65]

Because privacy gives us a choice over whom we share information about ourselves with, it allows us to limit how far we disclose certain information – put otherwise, it allows us to 'hide'. But privacy is about much more than hiding. It is about creating a space where we have the freedom to exchange information, think and take decisions about our societies and how they are being run.[66]

### *I.C.ii.b: Why we need privacy to form opinions and make decisions: the science*

Privacy gives human beings freedom from social control. The philosophers Bentham and Foucault developed the idea that removing an individual's privacy, by placing them in a physical environment where they may be monitored at any time, is the most effective means of ensuring that this person will bring his/her behaviour in line with social rules.[67]

Studies in sociology and criminology demonstrate that surveillance of individuals in institutional settings, like students, prisoners or workers, does indeed tend to induce conformity with existing rules.[68] Lawyers, political scientists and philosophers have asserted that Bentham's and Foucault's hypothesis also holds true outside institutional settings, arguing that the phenomenon of social control applies to individuals in society at large.[69] But for the most part, these academic disciplines have relied more on their own expertly informed intuition (and a few references to the use of surveillance by totalitarian regimes), than on any empirical research to back up their claims.[70]

**[Social control, the spiral of silence and the chilling effect]**

*Research in the field of social psychology, which has gone mostly unnoticed by other academic disciplines interested in privacy, has delivered a mountain of empirical evidence proving that Bentham's and Foucault's theory does have more general application. Their experiments prove that human beings tend to conform to the rules and beliefs of society. This phenomenon is referred to as 'social control'. Individuals who feel that they are being watched are even more likely to comply with social expectations and to agree with the opinions of the majority.[71] This body of research proves that the pressure humans feel to conform is so great that the mere suggestion that we may be monitored causes us to change our opinions and behaviour to match social expectations. This is so even if we know that no one is actually watching, and even if the majority opinion is factually incorrect.[72]*

*Building on early research in the field of social psychology, scholars from the field of communications studies have carried out similar tests to examine whether the phenomenon of social control also applies to the way that political opinions are formed in societies. A significant body of research confirms that individuals tend to be unwilling to give their opinions on political questions if they think that these run contrary to the majority view. Scholars of communications studies label this phenomenon of self-censorship the 'spiral of silence'.[73] This largely corresponds to the idea of the 'chilling effect' used by lawyers and activists working on free speech and freedom of association and assembly, predominantly in the USA. The chilling effect refers to the tendency of individuals (in particular journalists and interest groups) to self-censor when they suspect that they may be subject to surveillance. Unlike the concepts of the spiral of silence or social control, the concept of the chilling effect was mostly based on common sense and anecdotal evidence rather than empirical support, until very recently.[74]*

The general rule that individuals conform to majority opinions is not absolute – otherwise, the rules and practices of our societies would not have evolved as they have. New ideas that may eventually change majority opinions begin with a minority who are not afraid to speak out and challenge majority-held views. Majorities change their opinions through a gradual process. Social psychology research has found that new opinions and ideas can cause the majority to change its opinions if the proposition in question is put forward consistently. If a minority is consistent in its message, it is perceived by members of the majority to be more confident and certain of its views. And as the minority grows, the minority's perceived competence – and hence their persuasiveness – grows too.[75]

Research by communications scholars on the spiral of silence gives us a clue as to where minority opinions come from. Studies have found that there is always a 'hard core' of individuals who are willing to speak out even if they are contradicting the majority-held view. This 'hard core' is formed by individuals who have a high certainty of the correctness of what they are saying. In contrast, those who are less certain about the correctness of the majority position are more likely to 'go with the flow'. That is, they have not actively and consciously evaluated and agreed with the majority position. Rather, they accept it and are unlikely to express a different opinion.[76]

Social psychology research explains that minorities (in this context, those holding a minority opinion) are regarded by the majority with disapproval and can be subject to aggression from the majority. Because of this, individuals in the majority are unlikely to immediately admit in public that they have been persuaded by the minority to change their opinion. Because individuals fear disapproval from the majority, they tend only to admit that they have changed their opinions in private.[77] Spiral of silence research explains that as individuals begin to feel that their opinion is gaining popularity, they become more willing to speak out in support of what they once saw as a minority view.[78]

## *Hard wired to fit in*

The tendency among humans to follow social conventions and conform to majority views seems to have become hard-wired in humans. Early social psychology experiments showed that individuals who express disagreement with the rest of their group become highly stressed because they fear disapproval and hostility from the majority.[79] Recent research incorporating brain scans into these experiments shows that when an individual expresses opinions or beliefs different from their peers, this actually activates part of the brain associated with negative emotions.[80] Research also suggests that the hormone oxytocin (responsible for stimulating bonding between sexual partners and mothers with their babies) motivates humans to cooperate with members of their group and follow group rules.[81] Put otherwise, it appears that humans have evolved to fit in and go along with the majority – probably because we depend for our survival and prosperity on being part of a strong and harmonious group. When we disagree with the majority, we risk being isolated from the group – formerly, this could have meant denial of group benefits like food, shelter and physical protection.

Even if a particular minority is unable to persuade the majority to adopt its position, the debate that takes place appears to result in better-quality decision-making. This is because those in the majority seem to take the time to evaluate the minority position and suggest adjustments to the majority-held opinion or rule. It seems that because individuals belonging to the majority do not feel threatened by the minority, they are more likely to actively engage in a cognitive process of evaluation – which can result in accepting the new view or suggesting ways of adjusting the majority rule to accommodate the objections of the minority that seem to be valid. In contrast, individuals who are part of the majority are more likely to accept the majority view without critically evaluating it. It has been suggested that this is because the stress that individuals feel when they challenge the majority makes it more difficult for the parts of the brain responsible for cognitive thinking to be activated – so individuals are more likely just to accept the majority view even if they have not actively or internally endorsed it.[82] Some social psychology research suggests that over time, majority views consolidate into permanent attitudes among individuals who did not necessarily initially agree with them, but have not been prompted by contradictory views to evaluate the majority position and actively make up their minds.[83]

Interestingly, this analysis seems to confirm the concept of the ‘moveable middle’ that is used by some activists to help design campaign strategies. Simply put, this idea postulates that there is often a group in society that strongly supports an idea, and another group that strongly opposes it. And then there are those in the middle who are not sure where they really stand but tend to stick with the prevailing majority view. It is this middle section of society that can be moved over to endorse the values put forward by activists.

### *I.C.ii.c: How the theory applies in practice*

Privacy is vital to democracy because it gives us the liberty to choose what we share about ourselves and whom we share this information with. Without privacy, our thoughts, ideas and opinions are open to anyone. And because we tend to fear going against majority opinions, without privacy we are reluctant to learn or communicate about ideas that challenge the views of the majority. Privacy allows us to share information and develop ideas freely because we can choose to limit our communication to those people with whom we feel comfortable expressing our views. This gives us the freedom to research, think and discuss freely without the pressure to conform to the majority view.[84]

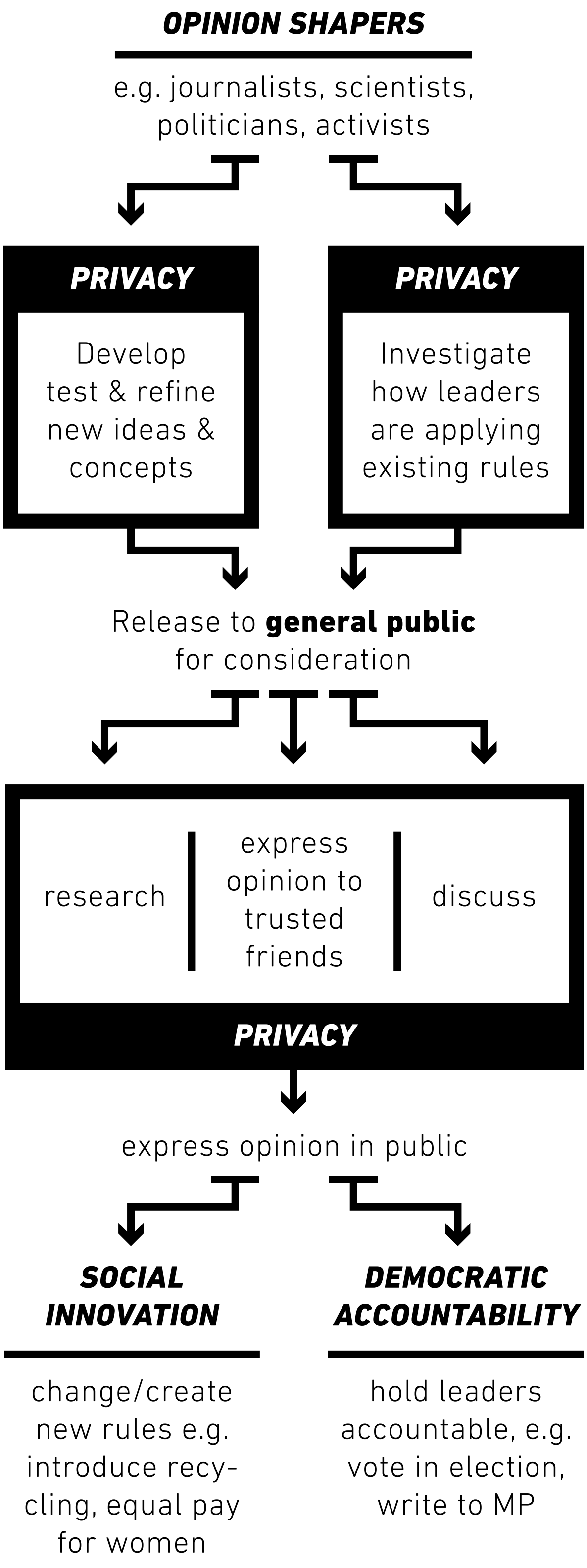
> **[Social innovation and democratic accountability]**
>
> *Privacy facilitates at least two democratic processes. First, the process of creating new or adjusting existing social rules, practices, laws and policies. I will refer to this as social innovation. Second, the process of evaluating whether power-holders (such as members of government or business or religious leaders) are applying existing rules properly. I will refer to this as democratic accountability.*

Privacy is important at two stages in the processes of social innovation and democratic accountability. First, to allow those people who shape opinions (by generating new ideas and information for discussion by the public) to develop, test and refine this information before sharing it. These opinion-shapers are referred to in spiral of silence research as the 'hard core' of individuals (noted above) who are so convinced of their opinions that they do not self-censor even in the face of a majority with a contrary opinion. Privacy also facilitates the second stage, which is when individual members of the public research, discuss and evaluate whether they want to reject or to act on the new ideas and information.

Put otherwise, opinion-shapers (such as academics, social commentators, journalists, activists or politicians) use privacy to create, test and refine new rules and concepts (social innovation) and to assess how existing rules are being applied by our political, commercial, religious and other leaders (democratic accountability). Many ideas that we now take for granted as valuable social or legal rules were once considered outrageous. For example, the abolition of slavery, racial equality, the criminalisation of domestic violence, the decriminalisation of homosexuality, animal welfare; or more recently, crowd-funding, the sharing economy, recycling, human rights, social media, freedom of information, globalisation, social entrepreneurship and environmentalism.[85] Opinion-shapers need space to research, test and refine ideas because, as noted, if minorities want to persuade the majority, their ideas must be convincing, well evidenced and presented consistently and confidently. Also, as noted, opinion-shapers need to be certain of the correctness of their ideas if they are not to self-censor due to fear of disapproval from a hostile majority.

Once opinion-shapers have tested and refined these rules, concepts and assessments privately, they can be released to the general public for consideration. As discussed, individuals are unlikely to publicly express support of minority ideas for fear of disapproval from the majority. That means that for individuals to learn about, evaluate and discuss opinions and information that challenge the majority view, they require privacy. If people progressively become convinced of (aspects of) new ideas or information, they gradually become ready to support them openly, which will lead to changes in majority opinion. Conversely, if minority opinions do not emerge to challenge majority views, then majority-held opinions gradually become more deeply entrenched among individuals who did not necessarily agree with them, but have not been prompted to critically evaluate them.

## PRIVACY & DEMOCRACY


OPINION SHAPERS
e.g. journalists, scientists, politicians, activists
PRIVACY
Develop test & refine new ideas & concepts
PRIVACY
Investigate how leaders are applying existing rules
Release to general public for consideration
research
express opinion to trusted friends
discuss
PRIVACY
express opinion in public
SOCIAL INNOVATION
change/create new rules e.g. introduce recycling, equal pay for women
DEMOCRATIC ACCOUNTABILITY
hold leaders accountable, e.g. vote in election, write to MP

This process allows new social norms to emerge or existing norms to be adjusted (which are often codified into laws and policies) and also for democratic accountability when the information being discussed relates to how existing norms are being applied by political, religious or business leaders. Because majority-held views become entrenched over time even among individuals who did not necessarily agree with them, if minority opinions become silenced, societies are less likely to make well-informed decisions about what laws or leaders they want. This is because fewer ideas and less information will be created by opinion-shapers for the public to debate, and the public will debate less. Unquestioned leaders are then more likely to make poor-quality choices that are based on majority opinions that have been formed with little critical evaluation.

It should be kept in mind that privacy's role in the democratic process is neutral, in the sense that it can allow both progressive and socially harmful ideas to persuade or influence majority opinion. Indeed, the process through which majority opinion is changed could be applied to partially explain the current trend of increasing xenophobia and racism – for a time considered unacceptable – in many European countries.

### *I.C.ii.d: How does this apply to mass surveillance?*

There is a growing body of research that examines whether the linked (perhaps identical) phenomena of social control, the spiral of silence and the chilling effect apply in the context of mass surveillance. As will be discussed below, surveys of public attitudes, experiments and other research on internet use and mobile phone use suggest that since the existence of mass surveillance programmes was revealed to the public, individuals see the internet and other communications tools as a place where they have no privacy. Many people feel that they have lost control over whom they share information with when they use emails, phone calls, text messages and social media. Because individuals now know that authorities can collect or are collecting all the information that passes over the internet, many people are beginning to behave as if the online world is the 'public' or the 'majority'. That is, individuals are starting to censor themselves and refrain from doing or saying things that might suggest they are deviating from prevailing social rules and political opinions. It should be noted that the opinion surveys and experiments concerning mass surveillance discussed below are based on public perception of mass surveillance. It seems irrelevant whether individuals believe that their information is actually being read or analysed. It is enough to make people self-censor if they simply think that their data is being collected. This suggests that even if lawmakers create limits on when collected data can be accessed by security services, this will not prevent self-censorship. This is confirmed by experimental research in the field of social psychology which shows that individuals are likely to become reluctant to air their views on controversial topics if there is a mere suggestion of surveillance.[86]

*How is mass surveillance affecting the creation of new ideas and information?*

Mass surveillance is making it much more difficult for new ideas and information to be developed and shared. Unfortunately, it is impossible to prove a negative – we cannot produce data on the number of news stories or innovative concepts that have failed to persuade the public of a new idea due to the social control/spiral of silence/chilling effect created by mass surveillance. However, there is plenty of evidence that journalists and associations are slowing down and sometimes stopping their work because mass surveillance removes the privacy that they rely on to do their job of informing the public and stimulating debate and change.

## Opinion-shapers self-censoring

Surveys of non-fiction writers and journalists have asked these groups about how they have changed their behaviour since the Snowden revelations explaining the extent of mass surveillance. A survey of around 500 journalists and non-fiction writers in 'free' countries (which includes all EU countries)[87] revealed that, because of mass surveillance: 20% have avoided writing or speaking on particular topics and another 14% have seriously considered doing so; 20% have avoided certain topics in phone and email conversations and 11% have seriously considered doing so; 31% have cut back or avoided social media activities and 11% have seriously considered doing so.[88] A survey by the same organisation focussing on the USA found that because of mass surveillance, journalists and writers were self-censoring on a wide range of issues – not only questions relating to national security, like military affairs. Topics that journalists reported avoiding included: Middle East affairs, mass incarceration, drug policy, pornography, the Occupy movement, the study of certain languages, historical issues like US preparedness for a nuclear conflict during the Cold War and criticism of the government.[89]

Another study based on interviews with journalists, lawyers and (former) government officials working on the intelligence community, national security and law enforcement in the USA shows that revelations about mass surveillance have made sources more reluctant to come forward to journalists, which makes it more difficult for the media to gather information and publish articles. Interviewees explain that whistleblowers are now far more reluctant to contact journalists about illegal or unethical behaviour. This is because whistleblowers fear that it is much harder for them to remain anonymous, since mass surveillance allows the authorities to search metadata to find out who has been in contact with journalists.[90] However, it is not merely whistleblowers working in the area of national security and law enforcement who have become reluctant to expose illegal or unethical behaviour. Even organisations working on completely unrelated issues have been negatively affected. For example, an organisation that promotes the privacy of patients' medical records, which relies on anonymous informants to report when corporations are breaking the law and illegally sharing patient records, reported a significant fall in the number of whistleblowers coming forward.[91]

A study of around 500 investigative journalists in the USA reported that, because of mass surveillance: almost 40% have changed the way that they communicate with sources; almost 50% have changed the way that they store and share potentially sensitive documents; almost 30% have changed the way that they communicate with other reporters, editors or producers; and 13% had decided not to contact a particular source.[92] While there has not been a similar survey for EU countries, associations of journalists have argued that mass surveillance makes it much more difficult for journalists to do their job because individuals are less willing to provide them with information due to the risk of revealing their identity.[93]

Mass surveillance is also interfering with the work of associations (particularly interest groups), which are important for democracy because they allow individuals to participate in politics by organising themselves to promote particular ideas, laws or policies. Associations in the USA have reported that their members have become reluctant to communicate with each other, organise or participate in activities because mass surveillance puts them at risk of revealing their identities and opinions.[94] These associations do not, for the most part, even campaign on security-related issues. Rather, their work is, at most, politically controversial, covering topics such as environmental protection, gun control, drugs liberalisation and equality. These associations have gone so far as to take legal action claiming that their right to free speech has been violated because of the chilling effect caused by mass surveillance.[95]

Mass surveillance is likely to interfere with the work of opinion-shapers in two different ways. As noted, opinion-shapers are likely to belong to the 'hard core' identified by spiral of silence scholarship who are sufficiently convinced of their opinions that they will not refrain from speaking out just because they are in a minority. But to become this 'hard core' who are resistant to social control/spiral of silence/the chilling effect, an opinion-shaper must first have been able to develop and refine his/her ideas to the point where he/she is confident and convinced of their correctness. Thus, the first way that mass surveillance may inhibit opinion-shapers is during the phase of idea development. Put otherwise, by removing privacy, mass surveillance may prevent opinion-shapers from being able to develop ideas and information.

Once opinion-shapers have developed their ideas enough to be so confident that they are resistant to social control/the spiral of silence/ the chilling effect, mass surveillance interferes in a different, more tangible way. At this stage, mass surveillance inhibits opinion-shapers indirectly because it makes them fear that they will be exposed and/or monitored, and that, as a consequence, some form of punishment will then follow.

Based on how others in a similar position have been treated, opinion-shapers will be aware that they run a real risk of sanctions. For example: whistleblowers have been disciplined, lost their jobs, prosecuted (and, in extreme cases, murdered); journalists have been placed on government watchlists and subjected to searches; journalists have seen their sources in third countries identified and harmed; members of civil society organisations (such as those campaigning on environmental protection, peace, anti-nuclear, civil liberties, equality and anti-apartheid) have seen their organisations and their personal lives infiltrated and destroyed by informants.[96]

It is likely that other categories of opinion-shaper are similarly deterred from developing and spreading their ideas. Academics, activists and politicians are likely to be aware of well-documented examples of their colleagues being placed under surveillance (usually illegally) and punished by the state for their unpopular political views. For example, academics in the USA and UK have been denied jobs, promotions or funding for research; activists (most famously, Martin Luther King) have faced blackmail and exposure of their personal lives to discredit or discourage them.[97] While there does not appear to have been a documented case of elected politicians being punished in this way for their 'unorthodox' views, British politicians from the Labour Party and Green Party who have been targeted by surveillance have complained that this makes them more cautious about expressing their views.[98]

*How is mass surveillance affecting the spread of new ideas and information?*

As discussed above, it is not only important that opinion-shapers be able to develop and refine new ideas and information before making these public. It is also important that members of the majority should be able to discuss, evaluate and decide on these new pieces of information and ideas. Mass surveillance is also interfering with this process because individuals are becoming less comfortable with communicating with each other over the phone, through email, social media or using the internet simply to inform themselves.

Recent surveys looking at how the public has changed its behaviour now that people are aware of mass surveillance suggests we are now more likely to conform to social conventions and majority opinions. Fifty-two per cent of respondents to a survey in Germany said that because of mass surveillance, they would probably refrain from using email or mobile phones to address potentially taboo questions, for example, to communicate with drugs counsellors, psychotherapists or marriage counsellors.[99] Twenty five per cent of respondents to a survey in the USA who were aware of the government's mass surveillance programmes said that they changed the way that they use technology to communicate, for example, by no longer discussing their private life online, using search engines to look for information on certain topics or making jokes that could be taken out of context.[100] This supports other research findings that report a drop of almost 30% in internet traffic to Wikipedia articles on almost 50 topics identified by US authorities as issues that they track on social media, following exposure of NSA surveillance programmes.[101] A 2014 survey that included four European countries showed that most people in the UK (60%), Germany (65%), Spain (66%) and France (76%) believe that the internet is not a safe place to express their opinions – in part because of government surveillance, and in part because of monitoring by businesses.[102] Two recent academic studies testing the spiral of silence and chilling effect theories confirm that individuals self-censor in their online behaviour because of mass surveillance. One study looked at the willingness of individuals to share their views on a story appearing through their Facebook feed. The research found that most individuals who perceived a risk of online government surveillance were less likely to share their views if they believed that these views were controversial.[103] Another study looked at the willingness of individuals to speak or write about certain topics online, engage in online searches, or share content they have created (presuming that these activities were legally permissible). 62% of respondents stated that they would be much less (22%) or somewhat (40%) less likely to speak or write about certain topics because of government surveillance. 78% agreed strongly (38%) or somewhat (40%) that government surveillance would make them more careful about what they discuss online. 78% agreed strongly (40%) or somewhat (38%) that government surveillance would make them more careful about what they search for online. 60% said that they would be much less (22%) or somewhat less (38%) likely to share content that they had created online because of government surveillance.[104] Thus, the academic research confirms that just like opinion-shapers, members of the general public censor themselves online and refrain from expressing political views that are not in conformity with dominant public opinion or accepted rules.

This means that the space for debate and discussion that privacy makes available is disappearing – because most of what we do involves using electronic devices, like phones or computers, from which governments collect information. Opinion-shapers are less likely to propose new ideas that challenge existing rules or collect new information that questions whether leaders are following the rules. And the public is less likely to be able to give these ideas or sources of information due consideration and make a free choice over which laws and leaders they want.[105] Mass surveillance poses a serious threat to the quality of decision-making in society and the ability of society to evolve and adapt to new circumstances.

### *I.C.ii.e: Rewriting the privacy argument*

The dominant approach among campaigners who have tried to explain the collective value of privacy has been to make the link with democracy without breaking down the mechanics of how humans use privacy to think and make decisions and without using existing empirical evidence to show how this process applies in practice. The absence of this kind of explanation can make it difficult to convince sceptical or undecided members of the public. The above analysis hopes to give campaigners new tools by drawing evidence from different academic disciplines to explain and clarify the link between privacy and democracy.

To reshape the public's understanding of privacy, the concept must also be explained more broadly than a right to individual secrecy, which has negative connotations and commoditises privacy. This section explained privacy as the freedom to think, form opinions and make decisions without social pressure or judgement. Privacy gives us freedom from social control because it allows us to choose whom we share information and opinions with. This allows us to create a space where we are free from external social pressure to conform to the dominant rules and ideas of our society. In this space, we can exchange sensitive information about ourselves, but also develop new concepts, form new opinions and test and improve ideas before sharing them. Opinion-shapers use this space to suggest new social rules or evaluate how the rules are being applied by our leaders. The general public uses this space to evaluate, accept or reject the information they receive, which allows either for the rules to be changed (social innovation) or for our leaders to be reprimanded for breaking those rules (democratic accountability). Mass surveillance removes the possibility to create these spaces because almost everything we do has some online component, and individuals treat the virtual world as a public sphere where there is no privacy.

Mass surveillance undermines social innovation and democratic accountability by fostering conformity with existing rules. If opinion-shapers are unable to propose new ideas or gather and share new information for the public to consume and judge, their societies will no longer be able to make informed choices about policies and laws, or when choosing their leaders and holding them to account. This has implications for democracy in general: governments are more likely to choose policies that sound attractive to the majority population, but that have not been adequately evaluated or refined; governments will feel even less of an incentive to act for the good of the population knowing that there are fewer critical voices to hold them to account. In the context of counter-terrorism, this makes it easier for governments to choose measures that have popular appeal, but that are ineffective or counter-productive in practice, because there is not enough freedom for opinion-shapers and the public to question these choices or hold leaders to account.[106]

# Part II: Ethnic profiling

The second counter-terrorism measure that this paper will examine is ethnic profiling. Authorities in many countries are using their powers, such as the power to stop-and-search persons, carry out border checks and raid properties, against individuals because they are (perceived to be) Muslim. In these situations, security services are generally using their powers predictively – to find potential terrorists who have not yet been identified by objective evidence. Because the security services do not know who they are looking for, they try to make an educated guess about potential suspects. So the authorities construct a profile and target individuals who fit the profile's criteria.

> **[Ethnic profiling]**
>
> *Ethnic profiling refers to a situation where security services are using their powers (usually predictively), using a profile that is based on ethnicity. That is, the security services have decided to exercise their powers in relation to an individual because of that person's ethnicity rather than basing themselves on objective evidence that proves the individual in question has acted unlawfully.*

To give a concrete example, law enforcement agencies may be of the opinion that drug dealers tend to be young black men dressed in sports wear. As a result, without any objective evidence, they routinely stop and search all teenagers wearing hooded tops who appear to be of African descent. Were it not for the fact that these individuals did not belong to this particular ethnicity, the security services would not have used their powers to stop and search them. If ethnicity plays a decisive role in the use of police powers, this amounts to unlawful discrimination.[107]

In practice, ethnic profiling is ineffective to prevent or detect crime and is a waste of resources.[108] Research shows that when police use ethnic profiling, they target a higher proportion of individuals from the 'suspect' ethnicity, and fewer individuals from the majority population or other minorities. In situations where law enforcement agencies have stopped using ethnicity as a criterion and instead used objective evidence of criminal activity, the results change significantly.[109] The overall number of searches or stops carried out by security services falls, the number of offences detected (i.e. the effectiveness of the stops) increases, and the disproportionality with which minorities are targeted compared to members of the majority population falls significantly.[110] Instead of basing themselves on ethnicity, which is not relevant to criminality, these security services use behavioural profiling. Behavioural profiles consist of patterns of behaviour that have been identified as suspicious, such as nervousness, avoiding eye contact, swapping bags with another person, travelling without luggage, purchasing one-way tickets with cash and repeated meetings between individuals within a short space of time.[111] Put otherwise, when using behavioural profiling, law enforcement officers are basing their decisions to stop or search an individual on the fact that the person is exhibiting suspicious behaviour – which is objective evidence.[112] Ethnic profiling is ineffective because it causes security services to focus their attention disproportionately on innocent individuals who belong to the targeted ethnicity, while suspects from the majority population escape scrutiny. It is inefficient because it results in fewer criminals being apprehended.

Profiling appears to be informing the use of preventive counter-terrorism powers, such as border control and police stop-and-search powers, in a number of countries.[113] As well as being ineffective to combat crime, available evidence suggests that ethnic profiling is also useless as a counter-terrorism measure.

## *Large scale ethnic profiling in Germany*

In Germany, after the 9/11 attacks, the authorities tried to identify potential terrorists by searching through several databases containing over 8 million people, such as social security registries, university records, the registry of foreign nationals and the records of phone companies.[114] The authorities highlighted people that matched the profile they had created of a potential terrorist: all Muslim males between 18 and 40 who come from certain Islamic countries and are current or former students. Over 30,000 individuals in the databases matched the search criteria. Their identities were then cross-checked against a database of two to three hundred thousand individuals certified to work in certain sensitive professions, such as pilots, airport workers or those dealing with nuclear energy or hazardous waste. The exercise failed to uncover any terrorist suspects and led to no charges being brought in relation to terrorist offences.

Similarly, in the USA in September 2002, the government implemented a 'special registration' programme targeting people 'deemed to be a risk to national security'. Individuals fitting the following profile were required to register with US immigration authorities and be fingerprinted, photographed, interviewed and submit to routine reporting: males of 16 and over from a list of over 20 countries with large Muslim populations. Almost 83,000 people living in the USA had registered by June 2003, after which much of the programme was phased out. It is thought that up to 5,000 individuals were temporarily detained under the programme and over 13,000 people deported for visa violations, but no one was charged with terrorism or terrorist affiliations.[115]

As of December 2016, French security services had carried out almost 4,300 police raids on homes and mosques and placed over 600 people under house arrest. However, this resulted in no prosecutions for terrorism charges.[116] While there have been prosecutions, it seems that a large proportion of these are for 'apologising for/praising terrorism', which would be legally protected as free speech in some jurisdictions.[117] Because of the low level of success, the fact that emergency legislation does not require police to provide objective evidence of suspicion as a condition for obtaining a warrant, and the fact that all those subject to raids were Muslims or people of Muslim appearance, the authorities have been criticised for basing their decisions on flimsy evidence (such as anonymous tip-offs from neighbours) and ethnicity.[118]

Profiling based on ethnicity is ineffective as a counter-terrorism tool because individuals involved with violent extremism related to Al-Qaeda and 'Islamic State' belong to a wide variety of nationalities and ethnicities – including increasing numbers of (white) Western converts.[119] Research suggests that Western converts are actually far more likely to resort to violent extremism than those brought up Muslim.[120] Ethnic profiling can actually create a blind spot for security services because they focus their resources on individuals belonging to the suspect ethnicity. Once recruiters and attackers become aware that the authorities are singling out certain ethnic minorities, they adapt their behaviour to avoid detection – for example, by choosing attackers from a different ethnicity.[121]

As well as wasting police resources and diverting attention away from potential perpetrators, ethnic profiling is likely to be counter-productive in the long run. It is well documented that innocent individuals who are subject to the use of police powers to stop-and-search or raid their property, feel humiliated and resentful when they believe that their ethnicity is the main reason they have been singled out. Individuals also report that they come to distrust the police and feel alienated and marginalised from their community and the nation. A further consequence appears to be an increase in discrimination and hate crime from the general public (which is often under-reported because of a lack of trust in police) that academics suggest results in part because racial profiling appears to legitimise discrimination by private individuals. This reflects the experience of members of Muslim communities targeted by security services in the USA, UK, and more recently Belgium and France. The destruction of trust in the authorities makes individuals less likely to cooperate with security services, for example by reporting suspicious behaviour or coming forward as a witness. The increased marginalisation and perception that the police cannot be relied on to protect their communities against discrimination and hate crime further compounds feelings of injustice and alienation from the nation, which plays a role in radicalisation, discussed below.[122]

As noted, obliging the security services to base their decisions on objective evidence, such as suspicious behaviour, can significantly reduce the number of innocent people targeted by intrusive law enforcement measures. In addition, this means that law enforcement officers will always be in a position to give a reasonable explanation to individuals as to why they have been subject to police powers. Research shows that when security services explain to individuals why they have been targeted, inform them of how to make a complaint and treat them in a respectful manner, then they are much less likely to have negative feelings about their encounter with police.[123]

# *Part III: What solutions should civil society organisations promote?*

This final section will outline measures that have proven effective in combating terrorism and which also either promote human rights standards, or can be calibrated to interfere with rights in a proportionate manner.

### *III.A: Invest in methods of intelligence-gathering that make us safer*

Rather than wasting public money on equipment and analysts for mass surveillance, governments should invest in methods of collecting intelligence that have proven effective. First, governments should increase the capacity of security services to carry out targeted surveillance of individuals whom they have reason to suspect of involvement with terrorism. As discussed above, in most cases security services have already been aware of individuals who have gone on to commit terrorist attacks. In these cases, resource constraints or poor communications within or between security services have prevented the authorities from stopping attacks. Put otherwise, the security services are doing their jobs, but they require more resources – including more staff – and improvements in how they share information. If governments also introduce measures to cut off the flow of people who are radicalised into violent extremism (discussed below), the number of individuals that the security services have to place under targeted surveillance will also drop in the long term.[124] Although targeted surveillance constitutes an interference with individual privacy, it can be justified in the interests of preventing crime and protecting public safety as long as safeguards exist to prevent abuse of these powers.[125]

Second, police use of stop-and-search powers, border checks or raids on homes and other properties should also be based on objective evidence rather than on the basis of ethnic profiling. In the context of stop-and-search powers, security services could copy successful use in the USA, Spain and the UK of behavioural profiling, including the introduction of 'stop' forms, training, monitoring the use of preventive powers for patterns of discrimination, and ensuring that the ethnic diversity of the national population is reflected in the diversity of security service personnel.[126] This would not only improve the efficiency and effectiveness of the security services – and thereby improve public safety – it would also remove a current source of mistrust and resentment towards the authorities (and one that contributes towards discrimination and hate crime which further alienates Muslims). In relation to the use of raids, security services should be required to prove the necessity of these measures to an authorising judge. This would help to reduce the number of innocent civilians targeted by these measures, which, again, constitutes a source of mistrust and resentment towards the security services and the state, a factor that increases vulnerability to radicalisation. In addition, when the security services use these powers, they should try to minimise the damage, trauma and humiliation involved by explaining their actions, using proportionate force and being as respectful as the circumstances permit. These measures will ensure that in the long run, the number of innocent targets is minimised, and that when an innocent person is targeted, their trust in and respect for the police is not damaged – which will help to facilitate cooperation with security services in the future, including for the purpose of gathering intelligence.

Third, governments should invest in the single most important source of information for security services: the general public, who routinely report suspicious activities to the police.[127] The failure of French and Belgian security services to predict and prevent attacks in 2015 and 2016 has been in part blamed on their failure to build relations with local communities, on whom police forces normally rely for information.[128] Conversely, police forces in a number of countries, particularly the USA and UK, have implemented models of 'community-oriented' or 'community-based' policing.[129] Although originally used to address high levels of crime among particular communities, it has now been adapted for use as a counter-terrorism measure in communities with high concentrations of Muslims. Research suggests that, if used as a trust-building measure, it can be an effective means of gathering intelligence and preventing marginalisation.[130]

The research broadly identifies two models of community-based policing. Some countries adopt a mix of these.[131] The community-targeted model is a top-down approach according to which security services try to recruit informants (sometimes against their will) from among the community, creating a network of local 'spies' who feed information to the police. Although this can generate intelligence for the security services, it also creates mistrust of the authorities and risks marginalising the community, which actually leads to less cooperation and information flowing between the community and the police in the long run.

Rather, the model preferred by researchers and advocated here is based on a mutually beneficial partnership between the police and the community. The community helps to determine what priorities police should address locally, becomes involved in policing (e.g. through neighbourhood watch programmes) and maintains a regular dialogue with local police. At a less formal level, police officers are expected to be present physically in the communities and become involved in community life. This should facilitate the emergence of genuine personal relationships and friendships and result in greater attention being paid to communities' day-to-day concerns, like petty crime or anti-social behaviour. Research suggests that this method of policing builds trust and then information flows voluntarily and organically from the community.[132] In essence, this is simply sensible policing, which should be applied universally and not just focused on particular communities as a counter-terrorism tool. If this tool is only applied to Muslim communities (as has been the case in the USA and the UK), this can lead to mistrust and suspicion, which can undermine its effectiveness.[133]

### *III.B: Self-help measures to protect privacy*

If governments cannot be persuaded to refrain from carrying out mass surveillance, a partial answer may lie in the use of encryption.

> **[Encryption]**
>
> *Encryption describes the process by which information, such as an email or credit card payment details, is made unrecognisable or scrambled when it passes over the internet.[134] Once the information reaches the intended recipient, for example a bank, or a friend's email address or phone, it is decrypted or decoded. This allows the recipient to read its contents. The information is decoded using an electronic key. This key can be held by the communications service provider, or it can be held on the devices of the individuals concerned – such as a telephone or computer.*
>
> *The most secure form of encryption is 'end-to-end encryption'. With end-to-end encryption, the electronic keys that can decode emails or other information are stored only on the recipient's phone or computer. This means that only the recipient's device can read this information. That is, the communications service providers – and the governments that obtain information from them – cannot decode this information.*

It has emerged recently that some communications service providers have cooperated with government mass surveillance programmes by providing customer data.[135] Several of these businesses have introduced encryption into their services to regain public trust.[136] In reaction to this, some governments are considering making end-to-end encryption impossible by obliging communications service providers to give the authorities encryption keys (known as a 'backdoor') so that they can decode information that these devices hold.[137] This is because security services argue that terrorists can prevent them from monitoring their communications and plan their attacks in secret by using encryption.

There are three problems with this argument. First, it is far from clear that encryption is a key tool through which terrorists avoid detection. For example, despite original speculation to the contrary,[138] during the Paris attacks, the perpetrators used non-encrypted mobile phones to communicate with each other.[139]

Second, even if communications service providers give backdoors to the security services, terrorists and criminals can still create their own encryption software or use software created in a country that has not made encryption illegal, for which the security services would not have backdoors. Furthermore, terrorists can (and still do) use older ways of communicating like couriers or code words in unprotected communications like text messages.[140]

Third, communications service providers and experts in the field agree that building backdoors for security services is dangerous because it is likely that terrorists and criminals would be able to steal the encryption keys and use the same backdoors. This would mean that internet services that rely on encryption, such as banking or payment systems or health insurance records, are no longer safe.[141]

It should also be noted that encryption does not disarm security services. The authorities can still use targeted surveillance (like bugging), or hack directly into the computer or phone of the target to read their communications once they have been decrypted or to obtain the encryption key.[142]

Although encryption can help protect privacy by hiding the content of communications, it does not tend to hide metadata.[143] By itself, therefore, encryption is not enough to counter mass surveillance. Ultimately, this means that the public will have to take steps to protect themselves from security services by using encryption software to conceal the contents of their communications, and other tools to anonymise their use of the internet and protect their metadata. It seems that most individuals, however, do not know about the existence of privacy tools or how to use them.[144] To that end, the population should be educated about and encouraged to use privacy tools. NGOs have been carrying out these activities.[145] However, NGOs should continue their efforts to press companies in the communications field to embed easy-to-use privacy tools into their software and equipment. This would reduce the amount of information these companies collect in the first place, and hence how much information the security services are able to obtain.[146] It will be difficult to better protect privacy until the general public becomes more aware of privacy tools and these tools are made much easier to use.

### III.C: Reduce vulnerability to radicalisation

As noted, in an effort to identify terrorists before they are known to security services, the authorities try to predict, by constructing terrorist profiles, whom to target and investigate. However, research (even by security services)[147] repeatedly confirms that it is not possible to draw up a profile of the 'average' terrorist. Among the violent extremists studied by various researchers, there is little consistency in levels of education, degree of religiosity, nationality, family situation, social background or past criminality. Increasingly, those involved in violent extremism include women, (white) converts and those in their teenage years (including children).[148]

> **[Radicalisation]**
>
> *The term 'radicalisation' may be problematic in itself because it lacks precise meaning and has been used to describe potentially conflicting explanations of why individuals turn to violence in pursuit of ideological goals. Broadly speaking, the phrase describes the process through which an individual embraces an ideology that justifies violence. The most commonly used understanding of 'radicalisation' refers to the final stages of indoctrination and emphasizes the role of the given ideology, such as a radical, inaccurate interpretation of Islam. A broader notion of the concept puts greater emphasis on contextual factors, such as social inequality, and sees ideology (religious, political or other) merely as a tool that helps to justify a break with generally accepted morality. This paper uses the broader notion of the term.*[149]

Authorities have also tried to identify the process through which individuals become radicalised into violent extremism that leads to terrorism.[150] Again, research shows that it is not possible to create a model that will allow the authorities to predict which individuals will radicalise, nor which, among those who are radicalised, will move from being non-violent radicals to violent radicals that engage in terrorism. However, it has been possible to identify the factors that make individuals vulnerable to radicalisation, as well as the different stages of the radicalisation process. Put otherwise, it is impossible to predict who will become radicalised into violent extremism, but we do know what factors increase the likelihood of it happening.[151] The present section concentrates on the phenomenon of 'home grown' radicalisation among people already settled in Europe and draws predominantly on two studies that review existing research on the issue.[152]

## The stages of radicalisation

The research shows that certain factors make individuals more vulnerable to radicalisation. To sum up: first, a sense of anger over an injustice which prompts an individual to question the existing order; second, a crisis of identity or purpose; third, the first two factors combine to create a 'cognitive opening' making the individual receptive to a new radicalising narrative; fourth, joining a network or group where individuals undergo mutual radicalisation usually under the supervision of a mentor or recruiter. The following paragraphs will explain these factors and how they fit together in greater detail.

Researchers have found that those who turn to violent extremism have experienced intense feelings of frustration and anger over an unjust or unfair situation, which causes individuals to question and want to change the existing social and political order. This can be rooted in a personal experience, for example: experiencing discrimination or hate crime; having one's social mobility blocked by being unable to get a job, or get a job commensurate to one's skills or qualifications. Anger and frustration can also be rooted in an individual's perception of unfairness towards others in the same group, for example: a perception that Muslims in Europe are living in relative deprivation (high rates of unemployment, petty crime, segregation, low levels of educational achievement, poor access to services) compared to the majority population.[153] A recurrent and powerful driver of resentment stems from the foreign policy of Western countries, which is perceived to be, first, directly attacking Muslims through military campaigns, especially in the Middle East, and second, collaborating with repressive governments. The poor treatment of refugees and migrants in many European countries is also regarded as another source of anger and frustration on which recruiters can capitalise.[154] It appears that most frequently, the perceived foreign and domestic victimisation of Muslims combine to exert a strong sense of outrage. This can also combine with a crisis of identity and belonging (religious, national or inter-generational) or purpose (due to lack of education or employment) that is reported sometimes among Muslim youth.

It is inaccurate to say unemployment, discrimination, or foreign policies that violate or support violations of human rights cause individuals to become terrorists in a simple causal process. While many Muslims perceive these injustices, only a tiny fraction become radicalised and an even smaller number turn to violence. Rather, what these factors do is to make it more likely for people to question the current social, economic and political order. These factors can also make it more likely for identity crises to emerge, especially among youth, who do not wish to identify with their parents, but who are also less likely to identify with a country that seems to have turned its back on them and is attacking Muslims worldwide.

The research suggests that the above factors combine to create some individuals who are angry and without a strong sense of identity, and that this leads to a 'cognitive opening' that is exploited by recruiters. A recruiter or mentor is able to explain the current social and political order as one where Muslims are violently repressed, subjugated and humiliated by Western powers in the Middle East, and then abandoned to socio-economic stagnation, discrimination, violence, suspicion and police harassment at home. Using a ready-made, well-structured meta-narrative based on selective and twisted interpretations of holy texts, mentors or recruiters then explain these injustices in absolutist terms, as a conflict between Islam and a morally bankrupt Judeo-Christian West. Radicalisation gives individuals a purpose (to fight for Islam), an identity (a jihadi) and a new family (fellow fighters).

Research also tends to agree that the stage at which individuals embrace extremism and later (perhaps) violence usually occurs in groups and networks. These could be groups based on friendship, family or without pre-existing ties, and they could be physical or virtual. As the group isolates itself from the rest of society, the group's moral and ethical boundaries shift and members mutually radicalise each other, often under the supervision of a recruiter or mentor. There are various explanations of how members of the group jump from being non-violent to violent extremists, including a personal catalyst event, such as a personal experience of hate crime.

Experts agree that it is impossible to find a direct causal link between any one of the factors mentioned and radicalisation into violent extremism. Research – not only of jihadi Salafist terrorism but also terrorist groups in Italy, Germany, Northern Ireland and right-wing skinhead youth – suggests that the ideology itself is the least important of the all the factors discussed that may lead an individual to embrace violent extremism.[155] Furthermore, different factors have different impacts, depending on an individual's circumstances. For example, some violent extremists are well educated, and these individuals often find their way into leadership positions or in operational roles in terrorist organisations where skill and intelligence is required to carry out complicated missions. University education may have been a factor in their radicalisation, either because this was the forum where individuals formed networks, or because it became a source of anger and frustration when individuals were not able to have the job or standard of living that an education should have opened to them,[156] or (some suggest) because of an individual's choice of degree.[157] Similarly, relative deprivation, neighbourhoods with high crime rates or poor services and communal facilities and high unemployment rates can become a factor in radicalisation because they support the narrative that Muslims are victims of discrimination and that the state has abandoned them. This can be a source of frustration and anger. But researchers also point out that these conditions create an environment where young people are bored, isolated and without a sense of purpose, which increases the appeal of extremist material on the internet in which recruiters promise status and adventure. Muslims in full-time employment or full-time education also seem more likely to have a stronger sense of national identity than Muslims who are not.[158] Finally, to the extent that socio-economic inequality contributes to criminal offending,[159] it increases the likelihood that individuals will spend time in prison, which is an increasingly important venue for radicalisation and the creation of jihadi networks.[160]

Governments have taken some steps to interrupt or reverse the end stages of the process of radicalisation, such as trying to stop the spread of indoctrinating material over the internet, challenging radical jihadi ideology, apprehending recruiters or implementing deradicalisation programmes.[161] But these measures target the very last stages of radicalisation into violent extremism. They are aimed at disrupting the ability of the radicalising narrative to exploit a 'cognitive opening'. And this cognitive opening was created by perceived injustices, frustration and lack of identity and purpose. These measures also target the least important of all the elements that may drive an individual towards violent extremism: the ideology.[162] There are two problems with this approach. First, to spot individuals who may be radicalising, the authorities need to apply intense scrutiny to Muslim communities. This in turn exacerbates feelings of mistrust and marginalisation that help make individuals vulnerable to radicalisation. The UK's 'Prevent' strategy has been repeatedly criticised on these grounds.[163] Second, governments are concentrating their efforts countering a specific extremist ideology rather than taking steps that could help to counter terrorism from all sources, including extreme left and right wing and separatist.[164]

In contrast, governments are doing very little to address the prior broader problems that create resentment, marginalisation and alienation in the first place. If governments were to implement their human rights obligations to promote racial equality, punish discrimination and hate crime, improve access to education and (non segregated) housing and take proper account of their human rights obligations in foreign policy,[165] this would reduce the likelihood that individuals would be vulnerable to radicalisation to begin with.[166] This is not to say that radicalisation would stop – there will always be individuals who can be persuaded to pursue violence. But by implementing human rights standards, governments will reduce the flow of new recruits, leaving the security services with a more manageable task.

# Conclusions

There is no inherent conflict between security and human rights. Governments have chosen to implement counter-terrorism measures that violate human rights standards because these offer voters the illusion of safety and the reassurance of strong, decisive leadership. But mass surveillance and ethnic profiling are making European countries more vulnerable to attack by misdirecting the resources of security services and undermining intelligence-gathering. Mass surveillance is also undermining democratic accountability and social innovation, which makes it more difficult for opinion-shapers and the public to influence and question the laws and policies the authorities choose to put in place. Longer-term failings to give human rights adequate importance as a goal of foreign policy and to promote racial equality and economic and social inclusion for minorities at home have helped create an environment conducive to radicalisation into violent extremism. Security services have failed to prevent attacks because they have not had enough resources or efficient methods of working that would allow them to carry out targeted surveillance and act on concrete intelligence. For our governments to make us safer, they must therefore properly resource law enforcement agencies to carry out targeted surveillance (with appropriate judicial and parliamentary oversight), invest in community-oriented policing and abandon ethnic profiling in favour of behavioural profiling. Combining these measures with policies to promote equality and inclusion for minorities, an ethical foreign policy, and existing measures to disrupt and reverse radicalisation would deliver long-term sustainable security.

This is not to say that the resolution to the purported tension between human rights and security is to co-opt human rights tools into counter-terrorism strategies. The argument made by the paper was not that human rights are valuable just because they are useful to combat terrorism. Rather, the paper has argued that if governments were to implement their human rights obligations, this would minimise the occurrence of threats to security and allow threats that do emerge to be dealt with more effectively. Put otherwise, human rights keep us safe.

# Notes

1 Israel Butler PhD (Nottingham), LLM (Nottingham), BA (Cantab). Israel Butler is Head of Advocacy at the Civil Liberties Union for Europe.

2 Lazarus, L. & Goold, B., 'Security and human rights: The search of a language of reconciliation', in Goold, B. & Lazarus, L. (eds.), 'Security and Human Rights', 2007, 1.

3 Rainie, L. & Maniam, S., 'Americans feel the tensions between privacy and security concerns', Pew Research Centre, 19 February 2016. For a summary of public opinion surveys in the UK post-Snowden revelations see: Cable, J., 'UK public opinion review: Working paper - An overview of public opinion polls since the Edward Snowden revelations in June 2013', 18 June 2015. For results of a survey concerning public attitudes across several countries, including six EU countries, see: YouGov/Amnesty International, 18 March 2015.

4 Haunss, S., 'Privacy activism after Snowden: Advocacy networks or protest?', in Fitz, K. & Harju, B. (eds.), 'Cultures of privacy – Paradigms, transformations, contestations', 2015, 227.

5 Consistency of message, as well as presentation of a credible alternative to the prevailing norm, plays an important role in determining whether minorities are successful in persuading majorities to alter their viewpoints. See overview of social psychology research by Maass, A. & Clark, R., 'Hidden impact of minorities: Fifteen years of minority influence research', 95 Psychological Bulletin (1984) 428.

6 Emerson, B., 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', UN Doc. A/HRC/31/65, 22 February 2016, 19-20; Coolsaet, R. '"All radicalization is local", The genesis and drawbacks of an elusive concept', June 2016, Egmont – The Royal Institute for International Relations, 41-42.

7 Greer, S., 'The exceptions to articles 8 to 11 of the European Convention on Human Rights', 1997.

8 For example, even if evidence showed that racial profiling was effective, because it undermines the core of the right to racial equality it would not be legally permissible. See: ECtHR, Application. No. 55762/00, *Timishev v Russia*, 13 December 2005, para. 58: 'the Court considers that no difference in treatment which is based exclusively or to a decisive extent on a person's ethnic origin is capable of being objectively justified in a contemporary democratic society built on the principles of pluralism and respect for different cultures'.

9 The paper does not deal with the use of personal data collected by businesses or the authorities that is then mined for profiling purposes to make commercial decisions or social and economic policy. For example, use of data for a purpose other than that for which it was collected, such as medical records being made available to insurance companies (for an alarming step in this direction in the UK see: New Scientist, 'Revealed: Google AI has access to huge haul of NHS patient data, 29 April 2016), or the aggregation of data from different sources that can result in erroneous and socially damaging outcomes for individuals or communities (like acting on tenuous correlations between certain characteristics and creditworthiness). These are genuine concerns, and they will be dealt with insofar as they are relevant to the use of terrorist profiles by security services. These problems relate more to the misuse of data that individuals have given over and the irresponsible use of profiling, rather than governments collecting all communications data through mass surveillance. For further reading on these issues see: Executive office of the president, 'Big data: Seizing opportunities, preserving values', May 2014; The Verge, 'The minority report: Chicago's new police computer predicts crimes, but is it racist?', 19 February 2014; Calders, T. & Žliobaite, I., 'Why unbiased computational processes can lead to discriminative decision procedures', in Custers, B. et al., 'Discrimination and privacy in the information society', 2013, chapter 3; Solove, D., '"I've got nothing to hide" and other misunderstandings of privacy', 44 San Diego Law Review (2007), 745; Lyon, D. (ed.), 'Surveillance as social sorting', 2003; Gandy, O., 'The panoptic sort: A political economy of personal information', 1993.

10 The Guardian, 'Fifteen secret warrants in force granting bulk data collection in UK', 7 July 2016; European Parliament Resolution, UN NSA surveillance programme, surveillance bodies in various Member States and impact on EU citizens' fundamental rights, 12 March 2014, P7_TA(2014)0230; Council of Europe, Committee on Legal Affairs and Human Rights, of the Parliamentary Assembly of the Council of Europe, Report on mass surveillance, 18 March 2015, Doc. 13734; Emmerson, B., 'Report of the Special Rapporteur on the promotion

and protection of human rights and fundamental freedoms while countering terrorism', UN Doc. A/69/397, 23 September 2014; The Telegraph, 'Germany, France and Spain "were spying on citizens"', 1 November 2013.

11 In cases of extreme urgency, it is possible for review to take place after surveillance begins: ECtHR, Application No. 37138/14, *Szabo & Vissy v Hungary*, 12 January 2016.

12 FRA, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Mapping Member States' legal frameworks', 2015, 17-18.

13 The Guardian, 'The Guardian guide to your metadata', 12 June 2013.

14 Schneier, B., 'The NSA doesn't need to spy on your calls to learn your secrets', Wired.com, 25 March 2015.

15 Mayer, J., & Mutchler. P., 'MetaPhone: The sensitivity of telephone metadata', Web Policy, 12 March 2014.

16 Lyon, D., 'Surveillance after Snowden', 2015, chapter 3; The Guardian, 'What can you learn about me from 24 hours of my metadata?', 3 December 2013; Zeit Online, 'Betrayed by our own data', 10 March 2011.

17 'Communications service providers' refers to companies that provide: internet services like Belgacom or UPC; mobile phone services like Orange or T-Mobile; phones and computers like Apple or Samsung; social media websites like Facebook or Twitter; email services like Microsoft or Google; or web browsers like Firefox, Safari, Chrome, or Internet Explorer.

18 Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58, OJ L 105, 13 April 2006, 54.

19 CJEU, Joined cases C-293/12 and C-594/12 *Digital Rights Ireland*, 8 April 2014.

20 CJEU, Joined cases C-203/15 and C-698/15 *Tele2 Sverige AB*, 21 December 2016.

21 Eurojust, 'Analysis of EU Member States' legal framework and current challenges on data retention', 26 October 2015, EU Council Doc. 13085/15.

22 Korteweg, D., 'Dutch House of Representatives passes dragnet surveillance bill', 16 February 2017, Bits of Freedom; Lubin, A., 'A new era of mass surveillance is emerging across Europe', 9 January 2017, Just Security; The Guardian, "Snooper's charter" bill becomes law, extending UK state surveillance', 29 November 2016; EUObserver, 'Belgium "insulted" by bad press on terrorism', 25 April 2016; Czuchaj, D., 'The new Polish Surveillance Act – back door for law enforcement', Lexology, 4 March 2016; ECtHR, Application No. 37138/14, *Szabo & Vissy v Hungary*, 12 January 2016; Krahulcova, L, 'We will, we will, watch you: codifying mass surveillance in France', Access, Now, 28 October 2015; BBC News, 'UK surveillance powers explained', 5 November 2015; Reuters, 'Dutch intelligence-gathering reform bill sparks privacy concerns, 1 September 2015; mano teises, 'Mindaugas Kiškis: Lietuvos kibernetinis saugumas turi būti užtikrintas proporcingomis priemonėmis', 12 March 2015.

23 Gallagher, R., 'Facing data deluge, secret UK spying report warned of intelligence failure', 7 June 2016, and documents published with this article: 'Digint imbalance', 7 June 2016; 'Digint narrative', 7 June 2016; 'Preston study', 7 June 2016.

24 Corrigan, R., 'Mass surveillance not effective for finding terrorists', 15 January 2015, The New Scientist; van Gulijk, C. et al., 'SURVEILLE Paper assessing surveillance in the context of preventing a terrorist act', 2014, 13-16; Goldacre, B., 'Datamining for terrorists would be lovely if it worked', 28 February 2009, Bad Science; Savage, S & Wainer, H., 'Until proven guilty: False positives and the war on terror', 21.1 Chance (2008), 59; Rudmin, F., 'Why does the NSA engage in mass surveillance of Americans when it's statistically impossible for such spying to detect terrorists?', 24 May 2006; Schneier, B., 'Why data mining won't stop terror', 9 March 2005, Schneier on Security.

25 Based on figures for the UK: The Times, '3000 terror suspects plotting to attack UK', 18 September 2015; BBC News, 'UK population "to top 70 million in 12 years"', 29 October 2015.

26 New York Times, 'Spy agency data after Sept. 11 led FBI to dead ends', 17 January 2006.

27 Solove, D., '"I've got nothing to hide" and other misunderstandings of privacy', 44 San Diego Law Review (2007), 745.

28 Balick, A., 'Internet privacy is about more than security: it's about psychology too', 27 July 2015; Pedersen, D., 'Psychological functions of privacy', 17 Journal of Environmental Psychology (1997) 147; Pedersen, D., 'Model for types of privacy by privacy functions', 19 Journal of Environmental Psychology (1999) 397; Rachels, J., 'Why privacy is important', 4 Philosophy and Public Affairs (1975), 323.

29 Rainie, L., Kiesler, S., et al. 'Anonymity, privacy and security online', Pew Research Centre, 5 September 2013;

30 For example, Abdo, A., 'You may have "nothing to hide" but you still have something to fear', ACLU, 2 August 2013.

31 Nucci, L., 'Culture, context, and the psychological sources of human rights concepts', in Edelstein, W. & Nunner-Winkler, G. (eds.), 'Morality in context', 2005, chapter 17; Jourard, S., 'Some psychological aspects of privacy', 31 Law and Contemporary Problems (1966), 307.

32 For example, Aiello, J. & Kolb, K., 'Electronic performance monitoring and social context: Impact on productivity and stress', 80 Journal of Applied Psychology (1995), 339.

33 New York Times, 'Racy photos were often shared at NSA, Snowden says', 20 July 2014; Washington Post, 'LOVEINT: When NSA officers use their spying power on love interests', 24 August 2013.

34 In this sense some have argued that privacy's main purpose is to conceal discreditable secrets: Posner, R., 'Privacy is overrated', Daily News, 28 April 2013; Posner, R., 'The right of privacy', 12 Georgia Law Review (1977), 393.

35 Wasserstrom, R., 'Privacy: some arguments and assumptions', in Schoeman, F., 'Philosophical dimensions of privacy: An anthology', 1984, chapter 14.

36 Research on public opinion in the USA shows that over the last ten years, support for surveillance has almost always been greater than opposition to surveillance. Support for surveillance does fluctuate: it rises when attacks occur and then drops off in the long run. However, the only time that public opposition to surveillance overtook public support for surveillance in the USA was just after the Snowden revelations in 2013. Rainie, L. & Maniam, S., 'Americans feel the tensions between privacy and security concerns', Pew Research Centre, 19 February 2016. For a summary of public opinion surveys in the UK post-Snowden revelations see: Cable, J., 'UK public opinion review: Working paper - An overview of public opinion polls since the Edward Snowden revelations in June 2013', 18 June 2015. For analysis of how public opinion towards counter-terrorism policies in Spain has varied in response to attacks see: El Pais, 'El 71% de los votantes del PSOE apoya el pacto antiterrorista', 19 February 2015.

37 For an instructive interview by Rights International Spain with Martin Scheinin, former UN Special Representative on counter-terrorism and human rights, covering several of the issues discussed below, see: Entrevista a Martin Scheinin, antiguo Relator Especial de la ONU sobre derechos humanos en la lucha contra el terrorismo, 29 June 2015.

38 Kirchner, L., 'What's the evidence mass surveillance works? Not much', 18 November 2015, Pro Publica; Privacy and Civil Liberties Oversight Board, Report on the telephone records program conducted under section 215 of the USA Patriot Act and on the operations of the Foreign Intelligence Surveillance Court, 23 January 2014; Bergen, P., et al., 'Do NSA's bulk surveillance programs stop terrorists?', January 2014, New America Foundation.

39 Readers may be aware of a recent independent assessment of the usefulness of 'bulk interception' in countering terrorism in the UK. The report found that 'bulk interception' had been 'vital' for 'counter-terrorism in the UK and abroad, cyber-defence, child sexual exploitation, organised crime and the support of military operations'. However, the report only examined 'bulk interception' directed at foreign-focused intelligence gathering. Thus, the report did not ask whether the retention of phone and email records and internet connection records by communications service providers could be considered useful, thus excluding a large amount of what is considered 'mass surveillance' from its assessment. In addition, the case studies concerning counter-terrorism examined by the report appeared to relate to intelligence gathering in areas of armed conflict, which meant that alternative means of getting information, such as targeted surveillance and human intelligence, were not available. See: Anderson, D., Report of the bulk powers review, August 2016, 20-21, 80-91. It should also be noted that former intelligence analysts have explained that it is technologically possible to obtain the same data without collecting such a large volume of information to begin with. This can be done by applying the filter

prior to (rather than after) the collection of the data. See e.g., Binney, W. et al., 'We could have stopped the Paris attacks', 23 November 2015, openDemocracy.

40 UK Parliament Joint Committee on the Draft Investigatory Powers Bill, Oral evidence, Jesper Lund, Chairman, the Danish IT Political Association, (QQ 234-249), 6 January 2016; Techpresident, 'In Denmark, online tracking of citizens in an unwieldy failure', 22 May 2013; Raab, C., et al., 'Increasing resilience in surveillance societies', 2013, 41-42; European Digital Rights, 'Shadow evaluation report on the Data Retention Directive (2006/24/EC) 17 April 2011, 13-15.

41 See, for example: European Commission, 'Evidence for necessity of data retention in the EU', March 2013. The report makes no effort to evaluate the anecdotal evidence provided by European governments.

42 The Telegraph, 'Only a fraction of terror suspects can be watched 24/7', 24 November 2014; BBC News, 'Terror watch lists: Can you keep tabs on every suspect?' 2 June 2013.

43 Gallagher, R., 'From Paris to Boston, terrorists were already known to authorities', The Intercept, 18 November 2015; ABC, 'Un inspector asegura que perseguían a varios de los acusados desde enero de 2003' 21 March 2007; Reinares, F., 'After the Madrid bombings: Internal security reforms and the prevention of global terrorism in Spain', Real Instituto Elcano working paper 40/2008, 14 October 2008; El Mundo, 'La Policía controlaba tres pisos del 11-M en vísperas de la masacre', 10 August 2005; Coroner's inquests into the London Bombings of 7 July 2015, Report under Rule 43 of the Coroner's rules 1984, 6 May 2011; Intelligence and Security Committee of Parliament, Report on the intelligence relating to the murder of Fusilier Lee Rigby, 25 November 2014; New York Times, 'Suspect held in Jewish museum killings', 1 June 2014; The Guardian, 'French suspect in Brussels Jewish museum attack spent year in Syria', 1 June 2014; Le Monde, '"Charlie Hebdo": quand la DGSI réécrit l'histoire', 3 April 2015; Wall Street Journal, 'Overburdened French dropped surveillance of brothers', 9 January 2015; The Guardian, 'French and Belgian intelligence knew Paris attackers had jihadi backgrounds', 16 November 2015; The Guardian, 'How the French intelligence agencies failed before the Paris attacks', 19 November 2015; Le Monde, 'Attentats de 13 novembre: quelles terroristes étaient déjà repérés?, 27 November 2015; Financial Times, 'Belgium admits mishandling Turkish terror warnings', 25 March 2016; RTBF, 'Faute de moyens, la surveillance des frères Abdeslam avait été abandonnée', 26 April 2016; Politico, 'Belgian police knew since 2014 that Abdeslam brothers planned "irreversible act"', 28 April 2016; Politico, 'Belgian police aborted Abdeslam investigation months before Paris attacks, media report', 17 May 2016; Flanders Today, 'Airport bomber monitored by police since last summer', 2 June 2016; Mail Online, 'MI5 missed chance to foil Paris and Brussels terrorists: Undercover operation was halted three months before meeting between ringleader and British extremists', 4 October 2016; The Guardian, 'MI5 opens inquiries into missed warnings over Manchester terror threat', 29 May 2017; The Telegraph, 'London Bridge attack latest: Terrorists named as police say they were not under surveillance as the posed "low risk"', 6 June 2017.

44 This seems to be because those who are self-radicalised are less likely to have come to the attention of security services by associating with other violent extremists. However, this is not always the case. For example, the individual who attacked the UK House of Commons in 2017 was known to the security services because he associated with extremists. See: The Independent, 'Khalid Masood: London terror attacker "was not lone wolf" but part of a wider conspiracy, security officials believe', 24 March 2017. Similarly, the individual responsible for the lorry attack on a Christmas market in Berlin had been under investigation for preparing an attack. See: BBC News, 'Berlin truck attack: Tunisian perpetrator Anis Amri', 23 December 2016. Sometimes an attacker is both known to the authorities for their extremist views and for mental health problems. See e.g.: New York Times, 'Suspect in Hamburg attacks was known to German police', 29 July 2017.

45 See: Europol, 'Lone actor attacks - Recent developments', 20 July 2016; Politico, 'Europol spotlights mental health in lone wolf attacks', 20 July 2016. News reports on lone actor attacks taking place after the publication of the Europol paper frequently note that the attacker had received treatment for mental illnesses: The Telegraph, 'Ali Sonboly: Everything we know about the Munich gunman', 24 July 2016; BBC News, 'Germany "was warned about Ansbach suicide bomber', 12 August 2016; DW, 'Alleged Düsseldorf ax attacker "apparently mentally ill", 9 March 2017.

46 UK Parliament Joint Committee on the Draft Investigatory Powers Bill, Oral evidence, William E Binney, retired Technical Director of the United States National Security Agency, (QQ 234-249), 6 January 2016; Binney, W. et al., 'We could have stopped the Paris attacks', 23 November 2015; The Intercept, 'Inside NSA, officials

privately criticise "collect it all" surveillance', 28 May 2015; Rowley, C., 'The bigger the haystack, the harder the terrorist is to find', The Guardian, 28 November 2014.

47 The Register, 'UK's internet spy law: 250m GBP in costs could balloon to 2 billion GBP', 6 November 2015; The Guardian, 'MI5's battle to identify radicalised Britons likely to turn to terrorism', 27 February 2015; Don'tspyonus.org, "Snoopers' Charter' could hit police forces with 1 billion GBP bill', 30 March 2016; Full Fact, 'The "Snoopers' Charter": what's the price of listening in?', 11 December 2012.

48 Large scale cyber-attacks hit many countries in May and June 2017: The Washington Post, 'Massive cyberattack hits Europe with widespread ransom demands', 27 June 2017; New York Times, 'Hackers hit dozens of countries exploiting stolen NSA tool', 12 May 2017; The Guardian, 'Cyber-insecurity is a gift for hackers, but it's our own governments that create it', 7 May 2017.

49 An example of information being held to ransom is when hackers use a virus to encrypt the data on or block access to a computer, requiring the victim (an individual, company or government body) to pay a fee for the data to be decrypted or to regain access to their computer.

50 BBC News, 'TalkTalk hack "affected 157,000 customers"', 6 November 2015; Wired, 'Hack brief: Hackers steal 15 million T-Mobile customers' data from Experian', 1 October 2015.

51 BBC News, 'Ashley Madison: what's in the leaked accounts data dump?', 19 August 2015; BBC News, 'Ashley Madison: "Suicides" over website hack', 24 August 2015; The Washington Post, 'Why the wife of a pastor exposed in Ashley Madison hack spoke out after his suicide', 9 September 2015.

52 Reuters, 'Yahoo says hackers stole data from 500 million accounts in 2014', 23 September 2016.

53 LinkedIn.com, 'Protecting our members', 18 May 2016.

54 AlJazeera, 'Facebook warns users of "state sponsored" hacking', 21 October 2015; Financial Times, 'MI5 warns universities on cyber spying', 10 April 2013.

55 The Guardian, 'US believes Russian hackers are behind Democratic National Committee leak', 27 July 2016.

56 Politico, 'Archuleta's out, but OPM's problems run deep', 7 October 2015.

57 AlJazeera, 'Bangladesh to sue US bank over $100m lost to hackers', 9 March 2016.

58 Big Brother Watch, 'A breach of trust: how local councils commit four data breaches every day', 11 August 2015; Big Brother Watch, 'NHS data breaches', November 2014.

59 Cyberstalkers have used publicly available information on the internet to track down and murder their victims. Mishler, J., 'Cyberstalking: Can communication via the internet constitute a credible threat and should an internet service provider be liable if it does?' 17 Santa Clara High Technology Law Journal (2000) 115.

60 For example, HRW & ACLU, 'With liberty to monitor all: How large-scale US surveillance is harming journalism, law and American Democracy', 2014.

61 For examples of attempts to make these broader arguments see: Xynou, M., 'Blog Series: Why shrugging at the Snowden revelations is a bad idea', Me and my shadow, Tactical Technology Collective, 24 October 2014; Carlo, S., 'Nothing to hide, nothing to fear? Think again', 23 July 2014; Greenwald, G., 'No place to hide: Edward Snowden, the NSA and the US surveillance state', 2014, chapter 4.

62 Rainie, L. & Maniam, S., 'Americans feel the tensions between privacy and security concerns', Pew Research Centre, 19 February 2016; Rainie, L. & Duggan, M., 'Privacy and information sharing', Pew Research Centre, 14 January 2016; Madden, M. et al., 'Public perceptions of privacy and security in the post-Snowden era', Pew Research Centre, 12 November 2014.

63 Nucci, L., 'Culture, context, and the psychological sources of human rights concepts', in Edelstein, W. & Nunner-Winkler, G. (eds.), 'Morality in context', 2005, chapter 17; Westin, A., 'The origins of modern claims to privacy', in Schoeman, F., 'Philosophical dimensions of privacy: An anthology', 1984, chapter 3.

64 Madden, M., Rainie, L., 'Americans' attitudes about privacy, security and surveillance', Pew Research Centre, 20 May 2015; Solove, D., 'Conceptualising privacy', 90 California Law Review (2002), 1087; Rosen, J., 'Out of context: The purposes of privacy', 68 Social Research (2001), 209; Schoeman, F., 'Privacy and social freedom', 1992, chapter 1; Altman, I., 'The Environment and

social behavior: Privacy, personal space, territory and crowding', 1975.

65 Kerr, I., & Barrigar, J., 'Privacy, identity and anonymity', in Ball, K. et al. (eds.), 'Routledge handbook of surveillance studies', 2012, 386.

66 Hughes, K., 'The social value of privacy, the value of privacy to society and human rights discourse', in Roessler, B., & Mokrosinska D. (eds.), 'Social dimensions of privacy: Interdisciplinary perspectives', 2015, chapter 12; Maras, M., 'The social consequences of a mass surveillance measure: What happens when we become the "others"?', 40 International Journal of Law, Crime and Justice (2012) 65; Magi, T., 'Fourteen reasons privacy matters: A multidisciplinary review of scholarly literature', 81.2 Library Quarterly (2011) 187; Westin, A., 'Privacy and freedom', 1967.

67 Lyon, D., 'The electronic eye: The rise of the surveillance society', 1994, chapter 4.

68 Staples, W., 'Everyday surveillance: vigilance and visibility in postmodern life', 2014; Subasic, E. et al., 'Leadership, power and the use of surveillance: Implications of shared social identity for leaders' capacity to influence', 22 The Leadership Quarterly (2011), 170; Cohen, S., 'Visions of social control: Crime punishment and classification', 2007; Tunnell, K., 'Pissing on demand: Workplace drug testing and the rise of the detox industry', 2004; Monahan, T. & Torres, R, (eds.), 'Schools under surveillance: Cultures of control in public education', 2010. A growing body of 'surveillance studies' scholarship emerging in the 1990s continues to catalogue the impact of surveillance technologies on various aspects of human life: Bell, K. et al. (eds.), 'Routledge Handbook of Surveillance Studies', 2012; see also successive volumes of the academic journal Surveillance & Society.

69 Gilliom, J., 'Overseers of the poor: Surveillance, resistance and the limits of privacy', 2001, 125-134; Reiman, J., 'Driving to the Panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future', 11 Santa Clara High Technology Law Journal (1995) 27; Benn, S., 'Privacy, freedom and respect for persons', in Schoeman, F., 'Philosophical dimensions of privacy: An anthology', 1984, chapter 8, 241ff; Gavison, R., 'Privacy and the limits of law', 89 Yale Law Journal (1980), 421, 448-455; Westin, A., 'Science, privacy, and freedom: Issues and proposals for the 1970's', 66 Columbia Law Review (1966), 1003, 1018-1020.

70 Only recently have legal scholars attempted to bridge the academic divide: Hughes, K., 'The social value of privacy, the value of privacy to society and human rights discourse', in Roessler, B., & Mokrosinska D. (eds.), 'Social dimensions of privacy: Interdisciplinary perspectives', 2015, chapter 12; Maras, M., 'The social consequences of a mass surveillance measure: What happens when we become the "others"?', 40 International Journal of Law, Crime and Justice (2012) 65. The truly ground-breaking leap by legal scholarship to present evidence from social psychology that backs up the link between privacy and democracy has been made only very recently: Kaminski, M. & Witnov, S., 'The conforming effect: First amendment implications of surveillance, beyond chilling speech', 49 University of Richmond Law Review (2015), 465; Penney, J., 'Chilling effects: Online surveillance and Wikipedia use', [2016] Berkely Technology Law Journal, 1, 28-29. It is perhaps because rights campaigners are often educated in academic disciplines like law, political science and philosophy that the rights movement has been unable to explain the connection between privacy and democracy by using empirical evidence. These academic disciplines are more accustomed to relying on theory rather than empirical research, and do not have a tradition of looking to other academic disciplines for help to support or challenge their own doctrines. As a (former) legal academic, the author recognises his own shortcomings in this respect. Until recently, because different academic disciplines have tended not to speak to each other, they were unaware that they might hold distinct pieces of a larger puzzle. While law and philosophy provide strong theoretical frameworks for privacy activists, social psychology and communications studies hold the empirical evidence to back up the theory.

71 Kassin, S. et al., 'Social psychology', 2011, chapter 7; Bordens, K. & Horowitz, I., 'Social psychology', 2014, chapter 7; Gerber, A. et al., 'Social pressure and voter turnout: Evidence from a large-scale field experiment', 102 American Political Science Review (2008), 33; Deutsch, M. & Gerard, H., 'A study of normative and informational social influences upon individual judgement' 51 Journal of Abnormal and Social Psychology (1955), 629; Bateson et al., 'Watching eyes on potential litter can reduce littering: Evidence from two field experiments', PeerJ 3:e1443, 2015; Fathi, M. et al., 'Effects of watching eyes and norm cues on charitable giving in a surreptitious behavioural experiment', 12 Evolutionary Psychology (2014), 878; Nettle D. et al., 'The watching eyes effect in the Dictator Game: it's not how much you give, it's being seen to give something', 34 Evolution and Human Behaviour (2013), 35; Nettle, D.

et al., '"Cycle thieves, we are watching you": Impact of a simple signage intervention against bicycle theft', 7(12) PLoS ONE e51738, 2012; Bateson, M., 'Cue of being watched enhance cooperation in a real-world setting', 2 Biology Letters (2006), 414; Sleek, S., 'Small nudge, big impact: How behavioural scientists are helping individuals – and societies – reach their goals', 26.7 Observer, September 2013.

[72] For example, in the 'watching eye' experiments discussed in articles cited in the preceding footnote, scholars found that simply adding an illustration of a pair of human eyes to a notice reminding or explaining certain rules (such as not littering or expected amounts of donations) made people more likely to comply. By way of example, many other experiments described in the literature in the preceding footnote have included placing the test subject among a larger group that was asked a series of questions with objectively right and wrong answers, such as identifying colours or the length of lines. In these experiments the 'majority' was secretly directed by the experimenters to choose an objectively incorrect answer. Experimenters would find that the 'innocent' subject of the experiments tended to go along with majority answers, even though these were wrong. Over time more sophisticated experiments have found that test subjects were also more reluctant to diverge from opinions that were expressed as a majority view.

[73] Noelle-Neumann, E., 'The spiral of silence: A theory of public opinion', 24 Journal of Communication (1974) 43; Glynn, C. et al., 'Perceived support for one's opinions and willingness to speak out: A meta-analysis of survey studies on the "spiral of silence."' 61 Public Opinion Quarterly (1997), 452; Scheufele, D. & Moy, P., 'Twenty-five years of the spiral of silence: A conceptual review and empirical outlook', 12 International Journal of Public Opinion Research, (2000), 3; Shanahan, J. et al., 'The spiral of silence: A meta-analysis and its impact', in Preiss, B. et al (eds.), 'Mass media effects: Advances through meta-analysis', 2007, 415.

[74] Penney, J., 'Chilling effects: Online surveillance and Wikipedia use', [2016] Berkely Technology Law Journal, 1, 28-29; Kaminski, M. & Witnov, S., 'The conforming effect: First amendment implications of surveillance, beyond chilling speech', 49 University of Richmond Law Review (2015), 465.

[75] Other factors also appear to play a role, such as whether the minority can present its message flexibly, how extreme the message is, whether the minority is perceived as self-serving, and the quality of the arguments used to back up their ideas. Dickel, N & Bohner, G., 'Minority and majority influence on attitudes', in Rossi, G., 'Psychology: selected papers', 2012, chapter 13; Maass, A. & Clark, R., 'Hidden impact of minorities: Fifteen years of minority influence research', 95 Psychological Bulletin (1984) 428.

[76] Matthes, J. et al., 'A spiral of silence for some: attitude certainty and the expression of political minority opinions', 37 Communication Research (2010) 774.

[77] Dickel, N & Bohner, G., 'Minority and majority influence on attitudes', in Rossi, G., 'Psychology: selected papers', 2012, chapter 13; Maass, A. & Clark, R., 'Hidden impact of minorities: Fifteen years of minority influence research', 95 Psychological Bulletin (1984) 428.

[78] Glynn, C & McLeod, J., 'Public opinion du jour', 48 Public Opinion Quarterly (1984) 731.

[79] Nemeth, C., & Wachtler, J., 'Creative problem solving as a result of majority vs minority influence', 13 European Journal of Social Psychology (1983) 45.

[80] Berns, G. et al., 'Neurobiological correlates of social conformity and independence during mental rotation', 58 Biological Psychiatry (2005) 245.

[81] De Kreu, C., 'Oxytocin conditions intergroup relations through upregulated in-group empathy, cooperation, conformity and defence', 79.3 Biological Psychiatry (2015) 165.

[82] De Dreu, C. & West, M., 'Minority dissent and team innovation: The importance of participation in decision making' 86 Journal of Applied Psychology (2001) 1191.

[83] Maass, A. & Clark, R., 'Hidden impact of minorities: Fifteen years of minority influence research', 95 Psychological Bulletin (1984) 428, 444-446.

[84] Haggerty, K., & Samatas, M., (eds.) 'Surveillance and democracy', 2010; Goold, B., 'Surveillance and the political value of privacy', Amsterdam Law Forum, 2009; Rouvroy, A. & Poullet, Y., 'The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy', in Gutwirth, S. et al., 'Reinventing data protection?', 2009, 45; Regan, P., 'Legislating privacy: technology, social values and public policy', 1995, chapter 8; Schwartz, P., 'Privacy and participation: Personal information and public sector regulation in the United States', 80 Iowa

Law Review (1994) 553; Gavison, R., 'Privacy and the limits of law', 89 Yale Law Journal (1980), 421, 455-456.

85 Richards, N., 'Intellectual privacy: Rethinking civil liberties in the digital age', 2015, chapter 6; Macklem, T., 'Independence of mind', 2007, chapter 3.

86 In this research the experimenters, who originally suggested that subjects' statements would be recorded, then announced that the equipment was broken and so there would be no record of what subjects said. Nevertheless, individuals still tended to self-censor and express socially accepted opinions. White, G., & Zimbardo, P., 'The effects of threat of surveillance and actual surveillance on expressed opinions toward marijuana', 111 Journal of Social Psychology (1980), 49. Similarly, see the 'watching eye' experiments: Nettle, D. et al., '"Cycle thieves, we are watching you": Impact of a simple signage intervention against bicycle theft', 7(12) PLoS ONE e51738, 2012.

87 According to the definition used by Freedom House. See Freedom House, 'Freedom in the World 2015'.

88 PEN, 'Global chilling: The impact of mass surveillance on international writers', 1 January 2014, 28-30.

89 PEN, 'Chilling effects: NSA surveillance drives US writers to self-censor', 12 November 2013.

90 HRW & ACLU, 'With liberty to monitor all: How large-scale US surveillance is harming journalism, law and American democracy', 2014.

91 Privacy and Civil Liberties Oversight Board, Report on the telephone records program conducted under section 215 of the USA Patriot Act and on the operations of the Foreign Intelligence Surveillance Court, 23 January 2014, 161-164.

92 Holcomb, J. et al., 'Investigative journalists and digital security: Perceptions of vulnerability and changes in behaviour', Pew Research Centre, 5 February 2015.

93 Reporters Without Borders, 'Reporters Without Borders Germany sues German foreign intelligence agency BND over communications mass surveillance', 1 July 2015; Committee to Protect Journalists, 'Groups call for EU action against mass surveillance', 1 August 2013.

94 Privacy and Civil Liberties Oversight Board, Report on the telephone records program conducted under section 215 of the USA Patriot Act and on the operations of the Foreign Intelligence Surveillance Court, 23 January 2014, 161-164.

95 Similarly, associations that have been subject to targeted surveillance in the past have also brought cases against the government alleging interferences with free speech because of the chilling effect (the tendency to self-censor) that results from surveillance. See: Ehlke, R., 'Political surveillance and police intelligence gathering – rights, wrongs and remedies', [1972] Wisconsin Law Review, 175.

96 BBC News, 'Berlin Brandenburg airport corruption "whistleblower poisoned"', 2 May 2016; The Guardian, 'Files detailing police spying operations against protesters published online', 14 January 2016; Ifex, 'Intelligence services tapped phones of 17 news agency journalists in Lithuania', 7 July 2014; BBC News, 'Police "spied on" Stephen Lawrence family, says Guardian newspaper', 24 June 2013; Evans, R. & Lewis, P., 'Undercover: the true story of Britain's secret police', 2013; Cunningham, D. & Noakes, J., '"What if she's from the FBI?" The effects of covert forms of social control on social movements', in Deflem, M. (ed.), 'Surveillance and governance: Crime control and beyond', 2008, 175; Ehlke, R., 'Political surveillance and police intelligence gathering – rights, wrongs and remedies', Wisconsin Law Review [1972], 175. In interviews with the author, NGOs from Hungary and Poland affirmed they believed they were under state surveillance and this surveillance alone appears to exert a mental strain on employees that acts as a deterrent for some staff to continue their work.

97 Williams, J., 'Academic freedom in an age of conformity: Confronting the fear of knowledge', 2016; The Guardian, 'MI5 spied on Doris Lessing for 20 years, declassified documents reveal', 21 August 2015; The Guardian, 'MI5 spied on leading British historians for decades, secret files reveal', 20 October 2014; The Guardian, 'Edward Snowden: US government spied on human rights workers', 8 April 2014; White, S., 'Academia, surveillance, and the FBI: A short history', in Deflem, M. (ed.), 'Surveillance and governance: Crime control and beyond', 2008, 151; Whitfield, D. & Landau, S., 'Privacy on the line: The politics of wiretapping and encryption', 2007, chapter 6; Garrow, D., 'The Martin Luther King, Jr., FBI file', 1984.

98 The Guardian, 'Police anti-extremism unit monitoring senior Green party figures', 28 April 2016; The Guardian, 'Public inquiry to scrutinise claims that policy covertly monitored politicians', 18 February 2016; The

Guardian, 'Police say they have not counted how many politicians they have been monitoring', 19 June 2014;

99 Forsa Institute, Meinungen der Bundesburger zur Vorratsdatenspeicherung, 17-28 May 2008.

100 Shelton, M. et al., 'Americans' privacy strategies post-Snowden', Pew Research Centre, 16 March 2015, 4.

101 Penney, J., 'Chilling effects: Online surveillance and Wikipedia use', [2016] Berkely Technology Law Journal, 1, 28-29. Penney points out (pp. 16-17) that this is a significant proportion of internet users, given that over half of internet users use Wikipedia as a source of information and it is one of the top ten most popular sites on the internet.

102 Globescan, 'BBC World Service Poll', 31 March 2014; BBC News, 'BBC poll: Web brings more freedom and more surveillance', 1 April 2014.

103 Stoycheff, E., 'Under surveillance: Examining facebook's spiral of silence effects in the wake of NSA internet monitoring', Journalism and Mass Communication Quarterly 8 March 2016 (published online ahead of print). For research on the 'spiral of silence' that results from social media more generally, see: Hampton, K., et al., 'Social media and the "spiral or silence"', Pew Research Centre, 2014.

104 Penney, J., 'Internet surveillance, regulation and chilling effects online: A comparative case study', Internet Policy Review (forthcoming, 2017).

105 Indeed, this is why totalitarian regimes such as Communist China, the Soviet Union and its former satellite states, as well as dictatorships in southern Europe and Latin America have used mass surveillance (through networks of informants and bugging phones and homes) to prevent their populations from challenging the social, cultural and political rules that kept the regimes in place. Kees, B. et al. (eds), 'Histories of state surveillance in Europe and beyond', 2014, chapters 4-8; Raab, C., et al., 'Increasing resilience in surveillance societies: Deliverable D2.2: The political perspective', 2013; 22-29; Raymond, M., 'Rejecting totalitarianism: Translating the guarantees of constitutional criminal procedure', 76 North Carolina Law Review (1998) 1193; Schwartz, P., 'Constitutional change and constitutional legitimation: The example of German Unification', 31 Houston Law Review (1994), 1027; Westin, A., 'Science, privacy, and freedom: Issues and proposals for the 1970's', 66 Columbia Law Review (1966), 1003, 1018-1020.

106 De Londras, F., 'Passing knee-jerk laws in the wake of terrorist attacks will not make us safer', 17 November 2015, The Conversation; Arman, A., 'Byproducts of Militarism and Terrorism', 28 December 2015, Foreign Policy Association.

107 FRA, 'Towards more effective policing – Understanding and preventing discriminatory ethnic profiling: A guide', 2010, chapter 2. This is not to say that ethnicity can never be used by security services. Ethnicity may legitimately form part of a suspect description if it is used together with other characteristics such as height, age, hair colour, and if it is based on objective evidence, like a witness statement. This can be referred to as legitimate criminal profiling. When ethnicity is the main or only reason prompting the use of police powers, in effect the security services are acting on a generalisation based on ethnicity rather than on objective evidence of an individual's criminal behaviour. See: Scheinin, M., 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', UN Doc., A/HRC/4/26, 29 January 2007, 6.

108 Open Society Justice Initiative, 'Ethnic profiling in the European Union: Pervasive, ineffective and discriminatory', 2009, chapter 3; Harris, D. 'Profiles in injustice: Why racial profiling cannot work', 2002, and Harris, D., 'Profiles in injustice: Why racial profiling cannot work', 2002 (video).

109 Put otherwise, the concept of 'reasonable suspicion' requires facts or information that would satisfy an objective observer that the person concerned may have committed an offence. See: ECtHR, *Gusinsky v Russia*, App. no. 70276/01, 19 May 2004, para. 53.

110 A study concerning Spanish police in Fuenlabrada shows that the number of people searched fell dramatically (from 408 per 10,000 residents in 2007 to 65 in 2013), the hit rate rose from 9% to 40% during the same period, and the disproportionality rate also dropped. See: Open Society Justice Initiative, 'Fair and effective police stops: Lessons in reform from five Spanish police agencies; Technical report', 2015. Research on the effect of replacing ethnic with behavioural profiling in US border searches shows that the number of searches at US borders fell by 75% and the rate at which offenders were detected rose from under 5% to 13% and became almost even for all ethnic groups – in contrast to 43% of searches being carried out on black people and people of Latino origin before behavioural profiling was introduced. See: FRA, 'Towards more effective policing – Understand-

ing and preventing discriminatory ethnic profiling: A guide', 2010, 36. The number of stops at UK borders fell from almost 90,000 in 2009 to around 34,500 in 2014, while the number of individuals detained rose from under 500 to around 1,300. This is attributed in part to the use of behavioural profiling. See: Anderson, D., Report of the independent review on the operation of the Terrorism Act 2000 and Part 1 of the Terrorism Act 2006, September 2015, 24-25.

111 FRA, 'Towards more effective policing – Understanding and preventing discriminatory ethnic profiling: A guide', 2010, chapter 3. Behavioural profiling has been criticized: New York Times, 'Racial profiling rife at airport, US officers say', 11 August 2012. However, this is mostly for the fact that it can be abused if officers fall back onto racial and ethnic stereotypes. Rather than objecting to behavioural profiling in and of itself, it probably makes more sense to take measures to deter security services from misusing their powers. For example, proper training, the use of stop-and-search forms and recording stops they make so that a superior officer can review these periodically. See also: Open Society Justice Initiative, 'Ethnic profiling in the European Union: Pervasive, ineffective and discriminatory', 2009, chapter 3; Harris, D., 'A good idea gone bad, part III: When behaviour profiling (good) leads to racial profiling (bad), 16 August 2012; FRA, 'Towards more effective policing – Understanding and preventing discriminatory ethnic profiling: A guide', 2010, chapter 4.

112 Schneier, B., 'Behavioural assessment profiling', 24 November 2004; Scheinin, M., 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', UN Doc., A/HRC/4/26, 29 January 2007, 16-17.

113 BBC News, 'Trump travel ban comes into effect for six countries', 30 June 2017; The Intercept, 'Complaints describe border agents interrogating Muslim Americans, asking for social media accounts', 14 January 2017; Washington Post, 'How Muslims are using social media to shame European cops', 15 February 2016; Washington Post, 'Racial profiling seems to be a weapon in Europe's war on terrorism', 15 February 2016; The Guardian, 'France awaits landmark ruling on "racial profiling" ID checks', 25 February 2015.

114 Berliner Zeitung, 'Die Telekon und die suche nach terroristen', 3 April 2009; BVerfG, Beschluss des Ersten Senats vom 04 April 2006 - 1 BvR 518/02 - Rn. (1-184), paras. 5-10; Kett-Straub, G., 'Rasterfahndung fällt durch das raster des grundgesetzes', Zeitschrift für Internationale Strafrechtsdogmatik 9/2006, 447, 449; Handelsblatt, 'ARD: Rasterfahndung hat keinen erfold', 9 April 2004.

115 Cole, D. & Lobel, J., 'Why we're losing the war on terror: Going on the offensive has only made us more vulnerable, 6 September 2007, The Nation; Cainkar, L., 'Post 9/11 domestic policies affecting US Arabs and Muslims: A brief overview', 24 Comparative Studies of South Asia, Africa and the Middle East' (2004) 245; Jachimowicz, M. & McKay, R., '"Special registration" programme', Migration Policy Institute, 1 April 2003; Cainkar, L., 'Special registration: A fervor for Muslims', 7 Journal of Islamic Law and Culture (2002), 73.

116 Human Rights Watch, 'Submission for the universal Periodic Review of France, January 2018', 29 June 2017; Liberation, 'Il faut avoir le courage de sortir de l'etat d'urgence', 13 December 2016. The majority of these were carried out in the first six week of the adoption of emergency legislation in November 2015: Leghtas, L., 'Dispatches: Will France's state of emergency ever end?', Human Rights Watch, 20 April 2016.

117 New York Times, 'Muslims in France say emergency powers go too far', 17 February 2016.

118 Muiznieks, N., 'Luttons contre le terrorisme dans le respect du droit', Le Monde, 3 February 2016; Amnesty International, 'Upturned lives: The disproportionate impact of France's state of emergency', 4 February 2016; HRW, 'France: Abuses under state of emergency', 3 February 2016.

119 The Guardian, 'Explainer: How and why Islamic State-linked rebels took over part of a Philippine city', 29 May 2017; BBC News, 'Philippines: IS-linked Maute group inmates freed in "raid"', 28 August 2016; Boutin, B. et al., 'The foreign fighters phenomenon in the European Union': Profiles, threats and policies', April 2016, International Centre for Counter-Terrorism; Europol, 'North Caucasian fighters in Syria and Iraq & IS propaganda in Russian language', September 2015; Di Ricco, M., 'Don't look for Latin American jihadis – yet', Al-Jazeera, 19 April 2015; Kleinman, S. & Flower, S., 'From convert to extremist: new Muslims and terrorism', 24 May 2013; The Guardian, 'Are converts more likely to be extremists than other Muslims?', 24 May 2013; The Scotsman, 'Al-Qaeda's white army of terror', 12 January 2008.

120 The Economist, 'Converts to Islam are likelier to radicalize than native Muslims', 1 April 2017.

121 This change in tactics is known as 'substitution'. Harcourt, B., 'Muslim profiles post-9/11: Is racial profiling an effective counter-terrorist measure and does it violate the right to be free from discrimination?', in Goold, B. & Lazarus, L. (eds.), 'Security and Human Rights', 2007, 73.

122 Amnesty International, 'Upturned lives: The disproportionate impact of France's state of emergency', 4 February 2016; HRW, 'France: Abuses under state of emergency', 3 February 2016; CNN, 'Why Belgium is Europe's front line in the war on terror', 24 March 2016; Washington Post, 'Racial profiling has destroyed public trust in police. Cops are exploiting our weak laws against it', 15 December 2014; Hakeem, F. et al., 'Policing Muslim communities: Comparative international context', 2012, chapter 3; Open Society Justice Initiative, 'Reducing Ethnic profiling in the European Union: A handbook of good practices', 2012, chapter 1; Spalek, B., 'Community policing, trust and Muslim communities in relation to "new terrorism"', 38 Politics and Policy (2010) 789.

123 The literature refers to this as 'procedural justice'. Bradford, B. et al., 'Police futures and legitimacy: Redefining "good policing"', in Brown, J. (ed.), 'The future of policing', 2013, chapter 6; Mazerolle, L. et al., 'Legitimacy in policing: A systematic review', Campbell Systematic Reviews, 2013.

124 See, for example, the multi-pronged approach in the UK: The Guardian, 'MI5's battle to identify radicalised Britons likely to turn to terrorism', 27 February 2015.

125 Such as requiring security services to obtain due legal authorisation from a judge or similarly independent authority, and periodic parliamentary review of how surveillance powers have been used. ECtHR, Application No. 37138/14, *Szabo & Vissy v Hungary*, 12 January 2016; ECtHR, Application No. 47143/06 *Zakharov v Russia*, 4 December 2015.

126 See sources discussed in relation to ethnic profiling, above.

127 For example, of 225 terrorism cases examined by US researchers, the single largest source of information responsible for triggering these investigations was information from the local community or a family member (17.8%), followed by information from an informant (16%). See: Bergen, P., et al., 'Do NSA's bulk surveillance programs stop terrorists?', New America Foundation, January 2014, 5. Both the former Commissioner of the Metropolitan Police in the UK and a parliamentary inquiry into UK intelligence services have stressed that community-based policing is indispensible because of the local intelligence it provides. Blair, I., 'The Tories' planned cuts to community policing will leave us at the mercy of Isis', 21 November 2015, The Guardian; UK Parliament, Intelligence and Security Committee of Parliament, 'Report on the intelligence relating to the murder of Fusilier Lee Rigby', 25 November 2014, 5.

128 Politico, 'Journey to Brussels' Terrorist safe haven', 27 March 2016; France 24, 'Paris attack probe turns to Belgium's "Islamist pit stop" of Molenbeek', 16 November 2015; Le Parisien, 'Jean-Pierre Havrin: "La police de proximité aurait pu repérer Merah"', 20 February 2015; La Capitale, 'Bruxelles: la police ne connait pas assez les quartiers, selon un rapport du Comite P', 28 December 2014.

129 The failure to prevent attacks in London and Manchester in 2017 was partly blamed on cuts to police budgets that meant that officers were no longer present in local communities and so unable to collect intelligence. See: The Guardian, 'Police cuts hit UK fight against terrorism, says former security chief', 6 June 2017; The Independent, 'I'm a serving firearms officer and the government is wrong to claim police cuts have nothing to do with recent attacks', 4 June 2017.

130 OSCE, 'Preventing terrorism and countering violent extremism and radicalisation that lead to terrorism: A community-policing approach', 2014; La Free, G., 'Policing Terrorism', 15 Ideas in American Policing (July 2012) 1; Spalek, B., 'Policing within counter-terrorism', Spalek, B. (ed.), 'Counter-Terrorism: Community-based approaches to preventing terror crime', 2012, chapter 3; Innes, M., 'Policing uncertainty: Countering terror through community intelligence and democratic policing', 605 The Annals of the American Academy of Political and Social Science (2006), 222; Haberfeld, M. et al., 'Terrorism within comparative international context: The counter-terrorism response and preparedness', 2009, chapter 2.1.

131 The UK's 'Prevent' strategy, for example, has provoked mixed reactions, as it crosses the line from community-focused to community-targeted (to the point of the ridiculous). Statement by the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association at the conclusion of his second visit

to the United Kingdom, 21 April 2016; The Guardian, 'Prevent strategy "sowing mistrust and fear in Muslim communities"', 3 February 2016; Huffington Post UK, '17 Signs you're a young person ripe for radicalisation', 22 July 2015; Huffington Post UK, 'Staffordshire University apologises for accusing student on counter-terrorism course of terrorism', 24 September 2015; The Guardian, 'School questioned Muslim pupil about Isis after discussion on eco-activism', 22 September 2015. For academic analysis see: Limbada, Z., 'Prevent and police-community partnerships in Birmingham', in Silk, D. et al. (eds.), 'Preventing ideological violence: Communities, police and case studies of "success"', 2013, chapter 8; Spalek, B., 'Community-based approaches to counter-terrorism', in Spalek, B. (ed.), 'Counter-Terrorism: Community-based approaches to preventing terror crime', 2012, chapter 2.

[132] Spalek, B., 'Community-based approaches to counter-terrorism', in Spalek, B. (ed.), 'Counter-Terrorism: Community-based approaches to preventing terror crime', 2012, chapter 2.

[133] Coolsaet, R. '"All radicalization is local", The genesis and drawbacks of an elusive concept', June 2016, Egmont – The Royal Institute for International Relations, 36.

[134] BBC News, 'Whatsapp adds end-to-end encryption', 5 April 2016; Wired, 'Forget Apple vs. the FBI: Whatsapp just switched on encryption for a billion people', 5 April 2016.

[135] For example, Yahoo: BBC News, 'Yahoo "secretly scanned emails for US authorities"', 4 October 2016.

[136] Sherwinter, D., 'Surveillance's slippery slope: using encryption to recapture privacy rights', 5 Journal on Telecommunications & High Technology Law (2007) 501. Communications service providers have at least two reasons for opposing mass surveillance. First, the loss of customers, as the public may decide to use different services that protect their privacy better. Second, the cost of collecting, storing and retrieving data when requested by the authorities. See, e.g. UK House of Commons, Joint Select Committee, Draft Investigatory Powers Bill Joint Committee: Apple Inc. and Apple Distribution International – written evidence (IPB0093), 21 December 2015; Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc. – written evidence (IPB0116), 21 December 2015.

[137] Tech Crunch, 'European MEPs want to ban states from backdooring encryption', 20 June 2017; The Bitcoinist.net, 'Amendment to ban end-to-end encryption passed by Hungarian parliament', 16 May 2016; The Guardian, 'French government votes to penalize smartphone makers over encryption', 3 March 2016; The Guardian, 'Cameron wants to ban encryption – he can say goodbye to digital Britain', 13 January 2013.

[138] The Telegraph, 'Mass surveillance can't catch terrorists. That's the uncomfortable truth', 16 November 2015; Forbes, 'Surveillance complex urged to "stop blaming cryptography for Paris attacks', 16 November 2015.

[139] Arstechnica, 'Paris terrorists used burner phones, not encryption, to evade detection', 21 March 2016.

[140] Time, 'Paris attacks fuel new debate on surveillance and encryption', 16 November 2016; BBC News, 'How to do terrorists communicate?', 2 November 2013. One should also consider that as surveillance technology evolves, so to do methods to evade that technology, though this tends to be difficult for the average person to access. See e.g., Russia Beyond the Headlines, 'Hiding from artificial intelligence in the age of total surveillance', 22 July 2017.

[141] Wired, 'After Paris attacks, here's what the CIA director gets wrong about encryption', 11 November 2015.

[142] Wired, 'After Paris attacks, here's what the CIA director gets wrong about encryption', 11 November 2015.

[143] Harvard University Berkman Centre for Internet and Society, 'Don't panic: Making progress on the "going dark" debate', 1 February 2016.

[144] Madden, M., Rainie, L., 'Americans' attitudes about privacy, security and surveillance', Pew Research Centre, 20 May 2015.

[145] See, for example: HCLU, 'Right to hide'; Tactical Technology Collective, 'Me and my shadow'.

[146] This is known as 'privacy by design'. See: Rubinstein, I., 'Regulating privacy by design', 26 Berkely Technology Law Journal (2012) 1409; Cavoukian, A., 'Privacy by design: Strong privacy protection – Now, and well into the future', 2011 Information and Privacy Commissioner, Ontario, Canada.

[147] The Guardian, 'MI5 report challenges views on terrorism in Britain', 20 August 2008.

148 Ahmed, M. et al., 'Milestones to militancy: What the lives of 100 jihadis tell us about a global movement', Centre on Religion and Geopolitics, April 2016; Boutin, B. et al., 'The foreign fighters phenomenon in the European Union': Profiles, threats and policies', April 2016, International Centre for Counter-Terrorism; New York Times, 'Who will become a terrorist? Research yields few clues', 27 March 2016; Vidino, L. & Hughes, S., 'ISIS in America: From retweets to Raqqa', December 2015; USA District Court of Oregon, *Latif v Lynch*, Declaration of Marc Sageman in opposition to the defendants' cross-motion for summary judgment, 7 August 2015; BBC News, 'Terror arrests reach record level, says Metropolitan Police', 14 May 2015; Bakker, E. & de Leede, S., 'European female jihadists in Syria: Exploring an under-researched topic', International Centre for Counter-Terrorism, April 2015.

149 See discussion of how the term has been used: Coolsaet, R. '"All radicalization is local", The genesis and drawbacks of an elusive concept', June 2016, Egmont – The Royal Institute for International Relations. Coolsaet suggests it is more appropriate to refer to a 'process of socialization into extremism that manifests itself in terrorism' (p. 37), because the term 'radicalisation' is generally understood only in its narrow sense.

150 The term 'extremism' has no commonly agreed definition. Most definitions of 'violent extremism' seem to boil down to the idea of ideologically motivated violence. Often violent extremism and terrorism are used interchangeably, though violent extremism may be taken to be a broader category that encompasses terrorism, but can also include individuals who support or promote violence, but do not commit violent acts themselves. For further discussion, see: Romanuik, P., 'Does CVE work? Lessons learned from the Global effort to counter violence extremism', Global Centre on Cooperative Security, September 2015.

151 After all, it is only a tiny fraction of individuals who are subject to the same factors that eventually become radicalised into violent extremism.

152 A systematic review of existing empirical research into the phenomenon of radicalisation in Western countries does reveal common ground among experts. A systematic review takes all existing research on a given subject, narrows down those studies that are of high quality, and then reviews all the evidence collectively to try to draw more general conclusions than the individual studies alone. Christmann, K., 'Preventing religious radicalisation and violent extremism: A systematic review of the research evidence', 2012. The findings of this systematic review are largely confirmed by another review of existing empirical and theoretical studies examining violent Islamic extremist movements globally. Denoeux, G. & Carter, L., 'Guide to the drivers of violent extremism', USAID, February 2009. Where the information in the following paragraphs does not derive from these two reports, or where additional information is available, supplementary references have been inserted as appropriate.

153 Europol, for example, suggests that high levels of economic and social inequality among parts of the Muslim population in France and Belgium helps to explain why Muslims in these countries have become more vulnerable to recruitment by violent jihadist groups than other European countries. See Europol, 'Changes in modus operandi of Islamic State (IS) revisited', November 2016, section 2.

154 Europol, 'Changes in modus operandi of Islamic State (IS) revisited', November 2016, section 5; BBC News, 'How attacks are forcing Germany to examine civil freedoms', 13 August 2016.

155 Coolsaet, R. '"All radicalization is local", The genesis and drawbacks of an elusive concept', June 2016, Egmont – The Royal Institute for International Relations, 24-29. Evidence suggests that those traveling to fight for Islamic State from Western countries have a rudimentary knowledge of Islam, which then makes them easier to indoctrinate. See: The Independent, 'Isis: Islam is "not strongest factor" behind foreign fighters joining extremist groups in Syria and Iraq – report', 16 November 2016.

156 Gambetta and Hertog argue that this plays a much greater role in non-Western countries which produce a high number of well-qualified individuals from privileged backgrounds who have no career prospects because of corruption, social blocking and a poorly performing economy. They, and the sources cited by the systematic reviews referred to above, suggest that because greater opportunities exist for university graduates in Western countries, university graduates are not represented as highly among violent extremists in the West. Of the samples examined by Gambetta and Hertog, only around 25% of Western violent extremists had a university education, compared to 42% in Saudi Arabia and 55% in the rest of the 'Muslim world'. See in particular chapter 3: Gambetta, D, and Hertog, S., 'Engineers of Jihad: The curious connection between violent extremism and education', 2016. Nonetheless,

it should be noted that even if university graduates in Western countries may not be blocked in their aspirations by economic stagnation and corruption, they do still face barriers from ethnic discrimination.

157 Recent research suggests that a disproportionately high number of individuals involved in violent extremism, both in the West and in countries with predominantly Muslim populations, are engineering graduates. Having accounted for other factors, the authors suggest that those who study engineering either already have or develop during the course of their engineering degree a particular mind-set that makes them prone to radicalisation into violent extremism. Gambetta, D, and Hertog, S., 'Engineers of Jihad: The curious connection between violent extremism and education', 2016.

158 Open Society Foundations, 'Muslims in Europe: A report on 11 EU cities', 2010, 76.

159 UNDP, 'Human development report for Latin America 2013-2014: Citizen security with a human face – Evidence and proposals for Latin America', 2013, chapter 2.

160 See statistics discussed by Gambetta and Hertog of violent extremists in Western countries: Gambetta, D, and Hertog, S., 'Engineers of Jihad: The curious connection between violent extremism and education', 2016, 64-65. A recent study of the 'global jihadi elite' (that is, including violent extremists who were born or grew up outside the West) found 65 of a sample of 100 had spent time in prison – a quarter of these had spent time in prison before becoming active jihadis. See: Ahmed, M. et al., 'Milestones to militancy: What the lives of 100 jihadis tell us about a global movement', Centre on Religion and Geopolitics, April 2016. See also: International Centre for the Study of Radicalisation and Political Violence, 'Criminal pasts, terrorist futures: European jihadists and the new crime-terror nexus', 2016.

161 Le Monde, 'Comment le gouvernement tente-t-il d'endiguer la tentation du terrorisme?', 10 May 2016; Politico, 'France to create anti-jihad rehab centres', 9 May 2016. See above for sources on the UK's 'Prevent' programme.

162 Coolsaet explains the shift in approach in Europe from an approach that would address broader root causes to an approach that concentrates on the final stages of indoctrination. He argues that an approach that addresses root causes is hard to swallow for most governments because it amounts to a 'whole-of-government' approach that tackles social inequality more broadly. Coolsaet, R. '"All radicalization is local", The genesis and drawbacks of an elusive concept', June 2016, Egmont – The Royal Institute for International Relations. This author would argue, however, that this is asking no more of governments than that they implement their already existing obligations under European and International Human Rights law to which they have voluntarily adhered.

163 BBC News, 'UN says Prevent extremism policy is "inherently flawed"', 16 June 2017; Committee on the Elimination of Racial Discrimination, Concluding Observations on the United Kingdom, 26 August 2016, UN Doc. CERD/C/GBR/CO/21-23, paras. 18-19; The Guardian, 'Prevent strategy "could end up promoting extremism"', 21 April 2016.

164 For a recent overview of terrorist attacks committed in Europe disaggregated according to cause (jihadist, extreme left, extreme right, separatist and single issue) see: Europol, 'European Union terrorism situation and trend report 2016 (TE-SAT 2016)', July 2016, annex 1.

165 On approach of using 'human development' as a means of fighting radicalization see: Taspinar, O., 'Fighting radicalism, not "terrorism": Root causes of an international actor redefined', 29 SAIS Review (2009) 75.

166 The European Commission appears to be trying to foster this broader view among national governments, though its most recent policy document suggests it places greater emphasis on disrupting radicalisation in its final stages, and its ability to address the social, economic and political background causes is limited. See: Commission Communication on supporting the prevention of radicalization leading to violent extremism, COM(2016) 379, 14 June 2016.

The Civil Liberties Union for Europe (Liberties) is a non-governmental organisation promoting and protecting the civil liberties of everyone in the European Union. We are headquartered in Berlin and have a presence in Brussels. Liberties is built on a network of national civil liberties NGOs from across the EU. Unless otherwise indicated, the opinions expressed by Liberties do not necessarily constitute the views of our member organisations.

***Website:***
liberties.eu

***Contact info:***
info@liberties.eu

***The Civil Liberties Union for Europe e. V.***
Prinzenstr. 103.
10969 Berlin
Germany

***Please consider supporting Liberties:***
https://www.liberties.eu/en/donate
IBAN: DE18 1009 0000 2679 5830 02
BIC: BEVODEBB (Berliner Volksbank)