# THE DITCHLEY FOUNDATION

## INTELLIGENCE, SECURITY AND PRIVACY

**14-16 May 2015**

**In cooperation with**

**The American Ditchley Foundation**

### Terms of Reference

A combination of renewed terrorism threats, rising cyber crime and fears of cyber attacks, and the Snowden revelations have put the on-line privacy debate back in political minds and on front pages: how can governments achieve the right balance between gathering enough information to keep their citizens safe, and those same citizens feeling that their privacy is being unreasonably invaded? Where should the line be drawn between individual rights and collective security? The debate has also brought to public attention the business model of the Internet whereby personal data is gathered by Internet companies and monetized for marketing purposes. Digital intelligence, whether by the State for security reasons or by the private sector for commercial gain, has raised concerns over personal privacy which governments and others are struggling to answer.

Even in the most open and democratic societies, people can have widely differing views. Some believe that upholding the law, saving lives and preserving national security is manifestly a top priority, that governments are only fulfilling their basic responsibility to their citizens in doing so, and that ordinary people have nothing to fear from checks designed only to root out those with something to hide. Others believe that this is a slippery slope, that the nature and availability of digital information makes it inevitable that governments, even apparently democratic ones, cannot be trusted not to abuse their powers and the information they collect.

The public discussion has focused very heavily so far on what happens in liberal democracies where the rule of law is seen as important. This is right and proper, but we should not forget that the situation is likely to be much worse in countries governed by authoritarian regimes where there is no scope for asking such questions, and where the risks to privacy and worse are likely to be much higher.

Another issue which deserves further exploration is what is meant by 'mass surveillance', with its connotation of repressive regimes spying on the population. Does the bulk access by agency computers to the large bearers of the Internet, in order to look for the communications of warranted targets, itself represent an intrusion on privacy, or do privacy rights become engaged only when a sentient human analyst is authorized to examine the material selected by computer? Under what circumstances should the police or intelligence agencies have access to metadata that can be derived from digital communications, such as the precise location of our phones or tablets and our Internet browsing history? Should there be additional protections for the privacy of our own citizens?

Democratic countries have evolved different ways of trying to ensure that their intelligence agencies are fully under democratic control, and reassuring ordinary citizens that they are not being unnecessarily spied upon. The Intelligence and Security Committee of the British Parliament published a long report in March 2015, setting out their conclusions after an investigation into British agencies' activities. They concluded that while the legal and political safeguards in the UK were broadly adequate, and the amount of British citizens' communications actually seen by the agencies was miniscule and properly authorized by ministers, the legal framework was nevertheless piecemeal, and the result was a lack of transparency which needed to be addressed. They therefore recommended a new and more comprehensive Act of Parliament to govern the agencies in future.

This report confirmed the judgements of an independent UK Court about the lawfulness of British interception practices, but some privacy campaigners seem determined to take their case further, to the European Court of Human Rights. The European Parliament and the UN Rapporteur are also engaged in the debate.

One key issue is who should be empowered to authorize interception of communications for crime-fighting or national security reasons. In the British case, for example, this is done by elected politicians, Secretaries of State, on the basis of submissions to them for permission by the agencies. The argument is that ministers, with advice from their officials, are best placed to judge the security, diplomatic and political contexts, and to assess the public interest as well as the lawfulness of the request. They can also be held accountable to Parliament and public for the decisions they take. Others believe that this role should be reserved for judges, who are less subject to political and other pressures, and to 'capture' by the agencies, and are better placed to judge objectively the necessity and proportionality of the request. Where does the balance lie here?

The right to individual privacy is a qualified right, in that it can be violated if there is an overriding public reason to do so. 2015 is the 800th anniversary of Magna Carta. That document influenced the drafters of the US Constitution whose 4th Amendment (1789) prohibits for US citizens unreasonable searches and seizures, and requires any warrant to be judicially sanctioned and supported by probable cause. The UN Declaration of Human Rights universalized this train of thought after the Second World War with the prohibition that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks'. The European Convention on Human Rights picked up this concept in the following terms: 'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

The legal test in UK legislation is that any intrusion has to be for a lawful purpose, and any action taken has to be shown to be both necessary, in the light of a known risk, and proportionate to the identified risk or threat. Is this a sufficient safeguard in practice? More widely, which country's laws and safeguards work most effectively, and which national practices might be of universal application? Conversely, where do the safeguards seem to be particularly inadequate, and why? We also need to bear in mind in all this that, while governance and oversight issues are for the most part nationally-based, the technological capabilities are potentially global, and the prospects for any kind of international agreements in this area close to zero.

Another basic question is who can be relied on to watch the watchers effectively? An arrangement such as the British one, where a statutory Parliamentary supervisory committee composed of senior Parliamentarians from both Houses of Parliament, including some former ministers, has the right of access to the information it requires from the Agencies, but does not have the right to reveal this information, requires a level of trust in the integrity and impartiality of the committee's members that not everyone is prepared to grant them. Similarly, the UK has very senior judges serving as Commissioners, supported by a team of specialist Inspectors, who have complete access to the Agencies and the police to assess compliance with the law. But, if we accept that secret agencies' work has to remain largely secret, by definition, to be effective, despite the far greater transparency about their existence and roles now than in the past, how is this to be dealt with? The agencies already complain that so much is now known about the way they operate that those responsible for security threats know what they have to do to avoid detection, for example using the so-called 'dark net', and that the security authorities are losing the battle. In this context, a particular issue arises about the role of the press. Who is to decide what can legitimately be revealed, and should journalists accept the implied position of complicity with the agencies if they are given privileged briefings? How are they to assess the truth of what they are being told when they can never be told the whole truth?

One question which has been posed in acute form concerns the rules and assumptions about friends and allies spying on each other. For example, were Germany and Brazil right to be so upset by the US behaviour revealed by Snowden? There is no doubt of the genuine depth of public and press anger in Germany and elsewhere about what they discovered, or that this has had significant effects on transatlantic and other relations, in the area of trade as well as security cooperation. Recent history gives a particular edge to German concerns. But was this really justified, or more a combination of naivety and hypocrisy, compounded by, for example, German and French agencies staying quiet about their own activities? Is the only real rule in this area not to get caught?

It is also legitimate to ask whether governments and their agencies really pose a bigger threat to individual privacy than the private sector companies operating in this space. Are people really aware of how much information about themselves they are volunteering when they use their smart phones; buy things via Pay Pal on eBay; tell the world their personal details on Facebook; comment on events on Twitter; and reveal their likes and dislikes via Internet searches, which can be tracked, analysed and the data sold on the open market? These sites collect more 'intelligence' on people than even the most invasive government, yet there are fewer calls to stop or control them, and fewer mechanisms too. Should there be stricter controls on what happens to this kind of data? How can we strike the right balance here between a wish to protect individuals' privacy, and the wider desire to maintain the web as an open global space, and avoid giving extra reasons to repressive governments to block sites and restrict reasonable content?

This is linked to an even more burning and difficult question. To what extent should there be an obligation on the private companies concerned to cooperate with governments seeking information for security purposes, and how transparent should this cooperation be? The companies' reaction to the Snowden revelations about the previous extent of their cooperation has been to strengthen end-to-end encryption of even routine communications, and reassure their users that they are no longer cooperating willingly, if they ever were. This has even become a matter of commercial attraction for customers worried about the use to which their own communications might be put. The agencies have responded with alarm to these developments, and are putting private, and increasingly also public, pressure on the companies to think again, and decide whether they really want to be complicit with terrorists using their systems to evade detection and to carry out attacks which could otherwise have been prevented, or with activities of serious criminals and child abusers. A separate debate is also going on about the extent to which some of the companies concerned have an obligation to ensure that their systems are not being used for recruiting and other purposes by social media-savvy jihadist groups, as the quantity and quality of such material have mushroomed, outstripping the ability of the authorities to detect it and take it down, despite increasing efforts to do so.

The hardest question of all is probably that of extra-territoriality and clashes of jurisdiction when individual countries legislate to compel Internet companies providing services in their jurisdiction to retain data and comply with warrants, but their requirements clash (such as the US First Amendment and EU Data Protection legislation placing differing requirements on US based companies). Countries with different judicial systems and repressive regimes will be quick to insist that provisions made by Western nations for the legitimate purposes of countering terrorism mean that Internet companies should respond to their own warrants, for example for information on dissidents.

This conference brings together a wide range of actors and thinkers from the intelligence community, as well as policy-makers, journalists, think tankers, and other experts from around the world to assess how best, in a democratic society, to strike the right intelligence, security and privacy balance. We will want to look particularly at questions such as the following:

## A Security needs and individual privacy

1. Is terrorism necessarily the threat which should be driving this debate, when it is arguably not an existential threat to our societies? How much should the threats from elsewhere, for example traditional espionage, cyber warfare and organized crime, be part of the discussion too?
2. At what point, if any, does the threat become so worrying that there is an overriding need to sacrifice some measure of individual liberties to keep ourselves safe? Are we at that point now, or are we at risk of voluntarily giving terrorists or others a victory over our values?
3. Is our privacy now seriously at risk from State surveillance, and are the public at large genuinely worried about this? Or is this largely the cause of a libertarian metropolitan minority?
4. Should we be ready to accept a higher risk of terrorism and cyber crime in exchange for greater preservation of Internet freedom? On what basis could such a judgment be made?
5. Are we being misled by the term 'mass surveillance'? Do individual citizens need to have privacy worries about intelligence agency computers accessing bulk bearers of Internet communications if what they are doing is sifting out and discarding all but a tiny proportion of the traffic likely to be carrying terrorist or other legitimate targets?
6. Is it still justified to treat access to communications data (who called whom, when and where) as a lesser intrusion into personal privacy than access to the content of our communications? How should we treat digital-age metadata (our browsing history, our electronic address book on our phones)?
7. Are intelligence agencies in democracies now operating with one hand tied behind their backs? Is there any hard evidence that laws and oversight regimes are hindering effectiveness?

## B Intelligence agencies and their supervision

8. Did the Snowden revelations show that intelligence agencies in some countries were out of control, or was this a misreading of the evidence?
9. How much do the public have a right to know more about the activities of their own intelligence agencies, or does this inevitably mean that their effectiveness is reduced? Has transparency gone too far or not far enough?
10. Who should authorize intrusive intelligence operations such as interception: politicians, senior officials or judges? Does it make a difference whether the purpose is to support a law enforcement investigation or intelligence for national security purposes? Should potential foreign policy fallout always be a consideration?
11. Is supervision of agencies' activities and monitoring compliance with legal regimes a parliamentary function, or a judicial one, or both/neither? Who should supervise the supervisors?
12. Should intrusive intelligence activity be the subject of specific national legislation? Can there be international norms between like-minded states to govern such activity?
13. To what extent should the citizens of a country (or those within its borders) have greater privacy protections than persons overseas (for example as provided for by the Fourth Amendment of the US Constitution)? Is spying on allies/friends/potential adversaries inevitable if there is a perceived national security interest?
14. How much should the press disclose about intelligence activity? Is the decision about what to print in the national interest one that only a free press can make? How do journalists avoid being 'captured' by agencies, and used by them to get out only the messages they want?
15. What do we know about safeguards (or the effect of their absence) in non-democratic societies?

## C The role of the private sector

16. Should we be worrying more about the intrusion of private sector service providers into our lives, the data they possess, and the use they make of it, than about government/agency activities?
17. Who should monitor and regulate the relevant activities of these companies, and to what extent is there a role for international agreements in all this? Are conflicts of jurisdiction inevitable (for example between EU and US law)?
18. Are we heading inevitably towards a fragmentation of the web, as some countries increase their efforts to control content and access, and worry about information held on servers outside their borders? Does the latter concern make any technical, economic or security sense?
19. Are the obligations and responsibilities of private sector companies above all to their customers, or are there 'national' security concerns which should override these in some circumstances?
20. How should we deal with global companies which increasingly have no national centre of gravity, and/or do not wish to be seen as having such a base?
21. What should be the nature of the security relationship between intelligence agencies and private sector providers, especially when they may in any case be cooperating against cyber threats in general? How transparent should these relationships be?
22. On whose side is the public likely to be in any trial of strength between governments/agencies and companies, for example, over access to data?