

**Privacy International Response to Home Office Discussion Paper:
Reconciling Security and liberty in an Open Society**



Submitted August 2004

Gus Hosein and Rosemary Walsh

Privacy International:

6-8, Amwell Street
Clerkenwell
London
EC1R 1UQ



August 31, 2004

The Home Secretary
Room 1019
50 Queen Anne's Gate
London
SW1H 9AT

Dear Sir

Please accept our submission in response to your Discussion Paper entitled

Counter-Terrorism Powers: Reconciling Security and Liberty in an Open Society

dated February 2004.

We welcome discussion on such an important set of issues. We also look forward to more discussion and deliberation in the future.

Sincerely,

Gus Hosen
Project Director
Terrorism and the Open Society
Privacy International

Rosemary Walsh
Legal Researcher

Privacy International, 6-8, Amwell Street Clerkenwell London EC1R 1UQ

Executive Summary

It is often said that the first duty of a Government is to protect its people. We believe that the first duty of Government is to govern itself, to conduct itself within the rule of law. We are concerned with many of the recent legislative developments in the United Kingdom, as they seem to be inimical to this view. In such times, we must ensure that Governments govern themselves with great care and provide security judiciously.

The creation of a regime of powers to combat terrorism, passed into law in times of emergency, may be a noble and urgent exercise. On occasion, the new laws created legal problems, some unforeseen and some that continue to be unspecified. In some cases, however, the Government has not acted in a noble manner, particularly in its responses to the Newton Committee's contestations.

The Privy Counsellors were charged, after some debate in the fall of 2001, to review the Act. They found many grounds upon which the Act and its implementation went too far. In its response, the Home Office repeatedly ignores or discounts the statements of the Newton Committee. This is not an acceptable form of review and oversight.

Repeatedly the Newton Committee identifies that powers proscribed in the Anti-Terrorism, Crime and Security Act 2001 (ATCSA) do not apply to terrorism, or should be restricted specifically to terrorism.

There are two common practices in combating terrorism through law. First is to consider terrorism within the existing criminal law regime. Some countries, most notably the United Kingdom, Canada, and the U.S. have decided that treating terrorism as a criminal act is insufficient. Instead a separate regime of law is created, granting greater powers to combat this most serious problem. After September 11 2001, these governments went about creating new laws under emergency circumstances to enhance the powers of the state, for the purpose of combating terrorism. The irony, however, is that these very same governments began treating all crime as terrorism by granting these powers to law enforcement authorities in all cases. This was not the intent of the law or the law-makers.

The Newton Committee noted this shift, and called the Government to task. In response, the Government is choosing to ignore the Committee's recommendations, to ignore the intent of Parliament, and to keep all these broadened powers at all costs. This is unacceptable.

We are concerned about the effect of anti-terrorism measures on criminal law. These concerns emanate very much from a procedural due process point of view specifically related to the means of obtaining evidence on certain individuals. Our general fear is that the special and legitimate powers employed by the relevant authorities in cases of terrorism and in a state of public emergency may be utilised in other areas of the criminal justice system in order to collate evidence to be used against 'ordinary' criminals. Safeguards that have been in place to preserve a person's privacy and integrity are there for a very good reason and should be rigorously maintained. It is therefore vital therefore that special powers used to combat terrorism can in no circumstances be used in the everyday operations of the criminal law.

We believe that it is better to have a separate system for dealing with terrorism, rather than merely using the criminal law, because combining the two systems is likely to produce abuses, intended or unintended, of special powers due to a potential blurring of the two systems. The strict use of a separate system for terrorism would also enable periodic utilisation. By this we mean that the special powers invoked at the time of a state of emergency can only apply to terrorism, and it is only during a state of emergency that they should and can be used.

By advocating a distinct set of legislation for combating terrorism, we are not diminishing the safeguards included in the criminal justice system. Instead, the principles and rules that apply in the latter can be used as a foundation for a system dealing with terrorism, such as those relating to the length of detention without trial. The benefits are an increased degree of certainty as to methods of dealing with terrorism and a transparent isolation of special powers. Importantly, it would allow for more effective prosecutions leading to a fair and impartial trial. We would however like to emphasise that where possible, the criminal law should always be used for as many instances as possible and resort to special powers should be kept to a minimum.

We would also at this point like to point out that in the United Kingdom, legal safeguards to protect privacy have already eroded much in recent years. Recent changes in criminal justice law, such as those within the Criminal Justice Act 2003, are reconsidering and renegotiating some of the most fundamental rights of due process. In a sense, all of this activity has left much to be desired for. And as such, there has been a chain of Court decisions with problematic implications for civil liberties. Much work needs to be done to fix this situation.

In this response to the Discussion Paper, Privacy International calls on the Government to acknowledge that the ATCS 2001 and other laws that were passed in the time after the atrocities of September 11 2001 went too far and took too much advantage in favour of law enforcement and abridged civil liberties and altered due process protections in law.

Most notably, we recommend changes in law, to:

- maintain strict boundaries between anti-terrorism and criminal law powers;
- fix rules on financial monitoring to reduce the collection of information on innocent individuals;
- revoke Part IV of ATCS as proposed by the Newton Committee and the Joint Committee on Human Rights, and to discuss feasible alternatives that accommodate the severity of the situation but maintain fundamental rights;
- carefully review interception powers and the use of intercepts as evidence in extenuating circumstances only, but with careful procedures;
- change all laws on the retention of fingerprints and other personal information unless there are charges involved, at a minimum;
- restrict the application of powers that affect public protest to situations involving terrorism;
- repeal provisions calling for data retention;
- and efforts to minimize or circumvent adequate scrutiny in Parliament should be removed from the law.

We understand that these are times of great duress and concern. We understand that much is being done by the Government to protect the country from future terrorist attacks. We also understand that this is a time for serious deliberation on where we are going with the decisions that were made in times of emergency.

And so, when the Government asks about the balance between liberty and security, the question is disingenuous. A genuine debate may occur on serious issues such as detention, which we recognize is a very difficult situation for the Government. But when previous safeguards against the abuse of powers or oversight provisions are curtailed, this is a mockery. Similarly, it is a mockery of the Parliamentary process when policies are pushed into anti-terrorism laws when there are no links to terrorism, even when these policies were previously rejected by Parliament. The retention of immigrants' fingerprints and the retention of traffic data are prime examples of this mockery of the emergency situations in the fall of September 2001. These powers to allow for the retention of personal information for the purposes of national security then permit the data to be used in just about any situation.

There was indeed a shift towards greater security after September 2001. Indeed, if there is another attack, the shift may go further. The Government must not interpret the public's interest in security as a *carte blanche* to increase all powers. We have already seen the rise of opposition in other countries, even those who also face the fear of terrorism each and every day. We have seen protests and laws countering anti-terrorism legislation when applied to sensitive personal information in the United States. We have seen public commissions inquire into gross exigencies in the deportation and treatment of Canadians. We have seen concern regarding the potential labelling of unlawful activities at protests as *terrorist activity*, and how this concern led to the failure of the Anti-Terrorism Bill in South Africa. The new Government in India is looking to repeal the Prevention of Terrorist Act, even as Malaysian Government is acting similarly. It is not as though these people are unafraid. These Governments are acknowledging that there are steps that go too far, despite great intentions.

Now is the time for reflection in the United Kingdom. If the Government does not reflect sufficiently, the United Kingdom may find itself even further out of step with the global community.

About Privacy International

Privacy International (PI) is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, police information systems, medical privacy, and freedom of information and expression. We are currently running research programmes on Freedom of Information, Terrorism and the Open Society, Watching the Watchers, and International Policy Dynamics. We have run highly popular public meetings on issues relating to ATCS 2001 and on the proposed identity system, most recently in October 2003 and May 2004. For more information please see our website at <http://www.privacyinternational.org>.

Specific Responses to the Discussion Paper

On Dividing Terrorism Law from Criminal Law

| | |
|-----------------------|--|
| Newton Recommendation | <p>"We think that it is an important principle that when we need special counter-terrorist legislation that provides for additional powers or departs from ordinary judicial procedures it should be kept separate from the body of mainstream crime and security legislation. This approach limits the impact on civil liberties and more readily allows for tailored safeguards and penalties to be provided."</p> <p>The Committee complained that during the passage of ATCS, the government argued against limiting the application of provisions to terrorist crimes, at the time stating that it could be difficult in practice to distinguish terrorist crimes from other crimes and so the powers in question should be available for all crimes. In response, the Committee claimed</p> <p>"Even were we to accept this argument (which was not emphasised to us during any of our evidence sessions), its limitations became clear to us when we discovered that some provisions of this Act had principally been used in cases clearly unrelated to terrorism, including sex offences and football hooliganism."</p> |
| Home Office Response | <p>1. Terrorism is a particularly abhorrent form of crime. The lack of any moral regard shown by terrorists inflicting loss of life, the terrorists' operations and their tight-knit associations means that is necessary, for as long as a threat exists, to have some exceptional legislation in place. However, much existing legislation aimed at combating organised crime is also helpful in the fight against terrorists who often rely on such methods to finance their activity. This is true of legislation bearing on criminal conspiracy and legislation about money laundering. Moreover, though differently motivated, terrorism involves acts which are already criminal.</p> <p>2. Against this background the Government does not believe that it would be an appropriate use of parliamentary time to re-legislate for provisions that Parliament has already passed.</p> |

The Home Office response makes the dangerous statement that since existing legislation can be used against terrorism, therefore there is no divide between criminal law and terrorism law. This argument justifies the continual use of terrorism law to combat regular crimes; which is unacceptable. These laws were passed with terrorism in mind, and in the case of ATCS 2001, in response to terrorism. To permit its application to non-terrorism situations is unacceptable.

Moreover, to excuse such a course of action on the needs of the parliamentary timetable is also unacceptable: an error was made in passing law in a time of urgency that can be used to combat criminal activity when this was not the intention nor the mood of the Parliament at the time; and this error must be rectified.

On Financial Monitoring

Orders to monitor financial activity can last for 90 days (up from 28) and require information to be supplied immediately by banks. This power was used only 8 times, and not since April 2003 (until the writing of the Committee's report in December 2003).

| | |
|-----------------------|---|
| Newton Recommendation | <p>Calls for reporting on the use of this power. "This provision created a power of significantly extended scope. We note that very limited use has been made of the orders. At present, banks are not able to process many types of information sufficiently quickly to meet the requirements of the orders, which raises questions about their utility."</p> <p>The reporting requirement is to aid the verification of whether there will be any further use of this power, "on the action that [the Government] propose to take to give them a realistic practical foundation."</p> |
| Home Office Response | <p>"The Government believes strongly that Account Monitoring Orders remain an important tool. Prior to the implementation of the Act, the financial services industry expressed concern over the extra workload the power could bring. Given this the police have taken care to ensure that the powers are used sparingly and in only the most extreme circumstances."</p> |

A statement of general care is insufficient compared to a call for reporting. Further oversight not only generates trust but also ensures accountability. We call for clear and regular reporting to Parliament.

On Failing to Report

There was previously an offence for failing to report to the authorities any information that has come to an individual in the course of business that leads him to believe or suspect someone of terrorist fundraising and money laundering.

ATCS 2001 makes it an offence for a 'regulated sector' to fail to report when they "know or suspect, or have reasonable grounds for knowing or suspecting" that such an offence has been committed; thus creating liability regardless of whether they had such a suspicion in fact.

| | |
|-----------------------|---|
| Newton Recommendation | <p>There have been no prosecutions for failure to report suspicious transactions. But there have been concerns from industry regarding difficulties of compliance, and the serious consequences that may flow from errors of judgement or even failures to notice." [from Carlile Report for 2001, p.19-20].</p> <p>The Committee argues that terrorist financing requires particular vigilance, tracking "multidimensional networks of transactions which, in themselves, may be entirely legitimate and unsuspecting." Concludes that "[t]his level of vigilance goes beyond the usual requirements in relation to "ordinary" financial crime.</p> <p>Calls for developing a mechanism for sharing more specific information on terrorist finance and reporting requirements developed between government and industry.</p> |
| Home Office Response | <p>"The Government acknowledges the importance of more effective sharing of information between the law enforcement authorities and the financial services industry. The police are now working closely with the financial services industry to develop more efficient and effective channels of reporting."</p> |

The Government must acknowledge and respond to the Committee's concerns regarding errors of judgement and limiting this surveillance capacity strictly to terrorist activity.

We also call for clear penalty regime for an abuse of the reporting by industry through using this data for other purposes, such as discrimination or generalised unsubstantiated surveillance.

We also call for clear and proportionate procedures to ensure that blanket indiscriminate surveillance is not being used by industry fearing accusations of inaction from government. We would like assurance that banking customers' privacy is being respected. This would include a notification requirement that records had been disclosed, allowing individuals to challenge the release, and a clear audit trail with reporting to Parliament on the use of these powers. We also call for a clearer delineation of the nature of the information that is disclosed, and some consideration should be given as to whether it is limited to the name of the account holder and the nature of any suspected illegal activity, so as to ensure proportionality and specificity.

Finally, we would like to see a clear audit trail to verify that information was not improperly accessed or misused. We would also like to see signs that there has been necessary and adequate training for those who are granted access to this data.

On Suspicious Activity Reporting

This covers the requirements on the financial sector to report activities that give rise to suspicion. According to reports, 100,000 such reports were expected for 2003; while only 63,000 were reported in 2002, and 15,000 per year prior to then.

| | |
|-----------------------|---|
| Newton Recommendation | <p>The Committee notes that this is similar to the provisions in the Proceeds of Crime Act 2002 that applies to money laundering; but also notes that the amount of reporting has been enormous. The Committee is concerned that there is no requirement to delete SARs in cases where the account-holder turns out to be innocent. The report notes that sometimes the grounds for SARs are not well-founded, and "There is a risk, therefore, that extensive financial information will be collected regarding completely innocent individuals." The Committee calls for an amendment to legislation to protect the privacy of innocent individuals and bodies corporate, by requiring the destruction of reports in cases where charges are not brought or are disproved. "An exception should be made only where appropriate authorisation is given that the report in question is material to an ongoing terrorist investigation."</p> |
|-----------------------|---|

| | |
|----------------------|--|
| Home Office Response | The Government does not agree with this recommendation. The law enforcement agencies have indicated that historical intelligence is often the main indicator of suspicious activity and this information will be lost if reports are destroyed. The power as it stands allows the law enforcement agencies to build and develop a detailed picture of suspicious activity over a period of time. Any material will be stored in line with the provisions of the Data Protection Act. |
|----------------------|--|

We find the Government's response to be wholly inadequate. A statement of usefulness is not sufficient to maintain such powers in an open society. Information, in the form of suspicious activity reports (SARs), are handed over to the government from private actors. This is a questionable transfer, as it is on awkward legal grounds as to whether this is state action or not. If it is state action, then the grounds for surveillance must be established more clearly. The Committee goes so far as to point to one case where a SAR was reported to be created on grounds that "I didn't like his attitude". This is insufficient grounds for intrusive government action.

For a government agency to hold on to this data, despite a declaration of innocence, is in contravention with human rights principles. If the grounds for collection of this data, being that it was found to be suspicious, no longer applies, i.e. charges have been dismissed or the action not deemed to be questionable after some scrutiny, a file should no longer exist. The creation of a database of arbitrarily-delivered SARs, where a proportion of these are found to be unnecessary SARs, and to keep this personal information indefinitely constitutes an arbitrary interference into the private life of an individual. The action clearly lacks specificity since the database contains information that is known to be inaccurate; this state action is disproportionate because it constitutes a vast database of arbitrary SARs to identify in a few cases, problematic activity.

Even with recent court decisions deciding that retention of information is lawful, they seem to indicate that as each SAR links to financial activity that provides a virtual current biography of the individual customers, then the law may frown upon such surveillance. In the case of fingerprints and DNA, these are pointers to evidence found on the scene of a crime. In *Regina v. Chief Constable of South Yorkshire Police*, Lord Steyn justifies the continued retention of fingerprints and DNA because the data collection technique "to eliminate those suspected or to incriminate others is enormous" due to the certainty of science. In SARs there is no such certainty -- rather once identified through uncertain criteria of having performed a suspicious activity and then cleared, an individual will always be in the database of those deemed suspicious until such a time that the State can make a case against the individual, and failing that, indefinitely. This is legally and morally unacceptable.

The Home Office has to work to legally resolve the concept of 'suspicious activity' as decided by a financial institution versus the legal concept of 'reasonable suspicion' prior to action by the police. In the situation of DNA and the fingerprint collection, an individual must be arrested for having committed a crime prior to the collection of such data (which we would say is already too low a standard). In the case of SARs, you are merely suspected by a financial institution under arbitrary criteria. Additionally, the mining and intelligence value of DNA and fingerprints is minimal in contrast to financial activity, which is informative, and biographic.

Based on the proportionality decision in *Regina v. Chief Constable of South Yorkshire Police*, where Lord Steyn claims:

- (i) the fingerprints and samples are kept only for the limited purpose of the detection, investigation, and prosecution of crime;
- (ii) the fingerprints and samples are not of any use without a comparator fingerprint or sample from the crime scene;
- (iii) the fingerprints and samples will not be made public;
- (iv) a person is not identifiable to the untutored eye simply from the profile on the database, any interference represented by the retention being minimal;
- (v) and, on the other hand, the resultant expansion of the database by the retention confers enormous advantages in the fight against serious crime. Cumulatively these factors suggest that the retention of fingerprints and samples is not disproportionate in effect.

and because in the case of SARs, the personal information is useful in itself, the information may be made public because it is stored by third parties and is disclosed to the police and is not protected as much by the police as fingerprint and DNA data, and the claim of the untutored eye does not apply because as many have claimed, the retention of such data does disclose substantial information regarding an individual; and as its

use is not just for serious crime, then the retention of this data (and retention of any form of data) is disproportionate.

We are also concerned that this information will be shared with foreign entities, again regardless as to status of guilt or innocence, considering the increased tendencies towards sharing information amongst other governments, based on Financial Action Task Force (FATF) initiatives, international agreements, and [EU draft council decisions](#).

Therefore we call for a clear set of procedures for the treatment of this data, how it is processed and analysed, and limiting the period of retention, particularly as this data is clearly sensitive and necessarily breaches the privacy of other individuals.

The manner in which the data is disclosed is also of concern. We would, at the very least, call for the approach established in Canada and its FINTRAC system. The set of transaction reports are stored by FINTRAC, and are then analyzed to determine whether there are links and patterns among individual transaction reports that appear to be suspicious, and other relevant data. When breaches of law are suspected, the Centre must disclose selected information to the appropriate law enforcement agency; the selected information is limited to the specific transaction. Written records must be kept to explain why the Centre decided to disclose the data to the law enforcement agency. Then the law enforcement authorities may seek a court order to obtain the rest of the information held by the Centre, on reasonable grounds to believe that an offence has been committed and that the information is likely to greatly assist in the investigation of the offence. (c.f. Auditor General of Canada. "Chapter 3: Canada's Strategy to Combat Money Laundering." Ottawa, 2003.)

On the Disclosure of Data

Within the ATCS 2001, information obtained by public authorities under statutory powers conferred for one purpose may be disclosed to the police and intelligence and security agencies to be used for completely different legitimate purposes; and can be shared internationally.

| | |
|------------------------------|---|
| <p>Newton Recommendation</p> | <p>The Committee notes that Part 3 of the ATCS 2001 was actually proposed in Part 2 of the Criminal Justice and Police Bill in January 2001, but was dropped due to concerns from the House of Lords. During the deliberations of ATCS, Parliament 'was given the impression by Government' that these powers "did not represent a substantial change, presumably on the grounds that information was already being disclosed in certain limited circumstances." The Committee notes that</p> <p style="padding-left: 40px;">"despite these instances of past practice and ministerial assertions to the contrary, these provisions are, in our view, a significant extension of the Government's power to use information obtained for one purpose, in some cases under compulsory powers, for a completely different purpose."</p> <p>As a result, this power "clearly falls into the category of mainstream legislation applicable to the investigation and prosecution of crime in general."</p> <p>Additionally, the claims by the Government that protections are offered by the Human Rights Act 1998 and the Data Protection Act 1998 "seems to us to be illusory since the burden will lie on the individual to complain about the disclosure of their confidential information in circumstances where, almost by definition, he or she will be unlikely to know that disclosure has occurred." The Newton Committee endorses the view that this is an invasion of privacy under Article 8 of the ECHR due to the range of offences covered, lack of statutory criteria to guide decisions, and the lack of safeguards.</p> <p>The Committee also argues that we need to monitor the disclosure by public bodies, how much and for what purposes, and including to overseas jurisdictions.</p> <p>The Committee concludes that new legislation is required to provide 'independent external oversight of the whole disclosure regime' so as to provide a safeguard against abuse and to ensure "that rigorous procedural standards governing disclosure are applied across the range of public bodies, prosecuting authorities and intelligence and security agencies. It should also require the independent overseer to publish statistics twice a year on the use of Part 3 (both within the United Kingdom, and to overseas authorities)."</p> |
|------------------------------|---|

| | |
|----------------------|--|
| Home Office Response | <p>The Government argues that oversight is already provided by the Data Protection Act 1998 and the continuing oversight of the Information Commissioner. The Commissioner has the duty, under s51 of the Act, to promote good practice and the power, under s40 of the Act, to take enforcement action for the breach of the data protection principles, which include the requirement that all personal data be "processed fairly and lawfully".</p> <p>The Government continues to say that</p> <p>"[t]he latest guidance on data sharing from the Department for Constitutional Affairs notes, in relation to public authorities generally, and statutory bodies like the Revenue Departments in particular: "Clearly, power to disclose personal information to prevent a crime may be implied if there is no express statutory power." This is consistent with the Government view, referred to by the Review at paragraph 160, that Part 3 did not break new ground in principle, whereas it does provide welcome clarity and precision."</p> <p>On the entire issue of reporting, the Government responds that</p> <p>The Government accepts the case that Revenue departments should include statistics on the use of Part 3 of the Act. Reports to Parliament already contain some statistics of the use of coercive measures of public interest, such as search and arrest.</p> |
|----------------------|--|

The Government's response is wholly inadequate, verging on obfuscation. The Newton Committee's demands are entirely reasonable: external oversight to safeguard against abuse with published findings. The Committee clearly states that protections offered by statutes (HRA and DPA 1998) are insufficient and 'illusory'. They call for pro-active protections, provided through oversight and reporting. This is because, despite false claims in Parliament, the powers in Part 3 of ATCS are new and expansive. The DPA and the Information Commissioner are not adequate.

We call for a review of these powers of data-sharing through informed Parliamentary debate, recalling that Parliament rejected these powers when they were not attached to an anti-terrorism law. We also call for it to be placed in primary legislation that is unrelated to terrorism, since clearly this power is not even nearly limited to combating terrorism. This is a sea-change in government policy achieved through a rushed response to terrorism, and is thus dishonest.

On Authorisation and Oversight for Data Disclosure

| | |
|-----------------------|---|
| Newton Recommendation | <p>The Newton Committee calls external oversight a "necessary safeguard, but it is not, in our view, sufficient." The Committee observes that intrusive powers usually are subject to judicial or independent warrants, particularly in cases when individuals are unlikely to know that such powers are being exercised.</p> <p>In cases involving terrorism, the Newton Committee accepts that internal authorisation by a senior person would be adequate for the disclosure of addresses or phone numbers. As for other crimes, the Committee calls for prior judicial approval "in any case involving less serious crimes or the disclosure of more sensitive information." And this will involve going back to Parliament: "Parliament should be given the opportunity to decide what level of authorisation should be required, depending on the seriousness of the crime and the sensitivity of the information being disclosed."</p> |
| Home Office Response | <p>Disclosure can only take place on the belief that it is proportionate to the aim being achieved. On the issue of warrants and the call for independent authorisation, however the Government responds:</p> <p>"The Government does not accept this view. The seriousness of the intrusion, how habitual it must be to serve the legitimate purpose it addresses, and whether the decision is usefully capable of prior judicial determination, are all material considerations about the balance to be struck between prior external safeguards, those internal to the public authority in question, and also judicial and other oversight."</p> <p>The Government argues that supplying information held by a public authority to another cannot "realistically be regarded as being as intrusive as, for example, a search of that individual's home."</p> <p>Given these considerations, and the numerous occasions where public sector data sharing of this sort, and joined up administration, will be in the public interest in promoting legitimate aims, the Government cannot accept the Review's proposal of prior judicial control of information disclosure.</p> |

We agree with the Newton Committee that this type of data disclosure is particularly dangerous because it involves vast amounts of information, and is used for purposes for which the individual never necessarily knows about. While the Government claims that this is not as invasive as a search of an individual's home, we would argue that because the individual never finds out, it is the equivalent of a secret search, and thus particularly pernicious.

We also agree with the Committee's claim that existing oversight is illusory due to the secrecy shrouding these data-sharing regimes. We do not see how a case can be taken through the courts under the Human Rights Act when we do not even know that information is being disclosed.

No matter what the Government claims regarding published guidance from the Department of Constitutional Affairs, these over-broad powers were unnecessarily included within an anti-terrorism legislation, and must be separated out and reconsidered. That the law was passed in response to September 11, after a previous failed attempt, and that the Government claims that it does not need external oversight nor independent authorisation is indicative of the fact that it does not want to deliberate openly on these issues. This is not how democratic institutions work.

On Detention, Derogation and Discrimination

The Newton Committee calls for the detention powers to be replaced as a matter of urgency, and to cease the derogation from the European Convention on Human Rights.

We firmly believe that such authoritarian power cannot be tolerated particularly in light of a lacuna of public information as to the safety and accountability of these individuals. Furthermore, in context, the detention of foreign nationals who cannot leave the UK does not sit comfortably with the requirement of Article 15, which permits derogations from the ECHR. This article requires that the measures, which are the subject of the application, must be 'strictly required by the exigencies of the situation' and the applicant country is in a state of emergency, which threatens the life of the nation.

It is our belief that the exclusion of UK citizens and the fact that detainees may be released if they are willing to return to their country of origin or to a third country contradicts the above mentioned conditions. Firstly, as the Newton Committee illustrates approximately 30% of arrests linked to terrorist activities are of UK nationals and so it is nonsensical to draw such a distinction between nationals and non-nationals. Secondly, if the exigencies of the situation require detention in the UK because the affected individuals represent such a threat to national security, once again it seems nonsensical to suggest that such a significant threat could diminish sufficiently once the person has left the country. If such wide gaps have been allowed to pass despite the UK's state of emergency, it is questionable whether these sweeping powers of detention are therefore also compatible with the doctrine of necessity. We propose that they are not; rather that the Government thinks it will minimise the controversy by bringing its actions within Article 5(1)(f) which allows for the lawful arrest or detention of a person "against whom action is being taken with a view to deportation or extradition". The word "lawful" should be noted here.

Further concerns regarding the legislation are the implicit derogations from Article 14, which protects the principle of non-discrimination, and Article 6, which ensure a fair trial. Most literature so far has focused largely on the derogation of Article 5. For derogations from the ECHR the contents must be specific in order for the derogation to be valid and it is our understanding that the UK Home Office has not explicitly referred to these Articles and furthermore provided information as to proposed safeguards in the absence of these rights. We are aware that the Court of Appeal has held that the legislation is not discriminatory but we find this incomprehensible considering that the provisions clearly discriminate against non-nationals because they lose their right to trial before prolonged detention whereas a UK citizen would undoubtedly have to be brought to trial before the option of detention could arise.

With regard to the issue of a fair trial we do not believe that the SIAC process qualifies as a fair and public hearing in that the standard of proof required for the procedure is much lower (reasonable belief and suspicion) than conventional UK trials. Fairness, in the administration of law, is a fundamental rule and should not be dismissed at any costs. The fact that detainees are at no point informed of the specific case

against them, which would allow them to formulate an explanation or defence, is atrocious. Their acting advocate, who once informed of the evidence may not confer with the client, is by no means a concession to the absence of judicial safeguards but rather borders on the farcical. ATCSA not only diminishes effective judicial review but also eliminates *habeas corpus*.

The Court of Appeal judgement (*A, B, C, D, E, F, G, H, Mahmoud Abu Rideh, Jamal Ajouaou v. Secretary of State for the Home Department*) on the 11th August 2004 states that the proceedings before SIAC are not criminal proceedings for the purposes of Article 6. We would very much like to take issue with this statement in that it leaves the detainees in a legal limbo. The intention behind Article 6 should be considered here, otherwise there is little point in ratifying such human rights conventions, as it is clear that Article 6 is intended for trials that will involve the detention of a person's liberty. While they may not strictly be criminal proceedings, in our estimations Article 6 and the European Convention of Human Rights are specifically designed to prevent injustices, and to evade responsibility through a façade of bureaucratic categorisations is damaging.

We therefore strongly support the revocation of Part IV of ATCS as proposed by the Newton Committee and the Joint Committee on Human Rights (JCHR), and would like to discuss feasible alternatives that accommodate the severity of the situation but maintain fundamental rights. We note furthermore that the U.S. and the UK are the only liberal democracies that see fit to incorporate powers of indefinite detention into the legislative framework. Whilst the Home Office has clearly taken the time to review and detail the actions of other countries in this regard, we find it insufficient that they did not comment on these other methods or justify why they were not potential options for Britain considering their less draconian approach. Whilst it is appreciated that some evidence may not be available in the public domain due to its sensitive nature, we hoped that the Home Office would have been slightly more informative as to its reasons for behaving differently to other European countries that may face similar threats, particularly in light of the document's status as a discussion paper.

It appears that many countries detailed in the Home Office Report and the eighteenth report of Session 2003-2004 of the JCHR, "Review of Counter Terrorism Powers" have extended their criminal laws in order to accommodate acts of terrorism. This undoubtedly represents a more favourable alternative to detention of individuals without charge in the fact that it draws individuals within the ambit of the law rather than in the limbo that the non-nationals may find themselves in within the UK. The option of adding a link to terrorism to an existing crime to administer greater penalties is appealing in that it reflects the increased severity of the illegal action.

Finally, whilst the issue of the legality of the derogation was not raised in the Discussion Paper, and we note that many organisations have taken this for granted; we would like to briefly comment on this issue. Whilst we advocate separate terrorism laws, we stress that these should only be used in a state of emergency. According to interpretations by the ECHR, this implies temporary measures that will protect the state from a threat that affects the life of the nation. Primarily, since 1974, the UK has consistently had special powers in place to deal with terrorism. Whilst cases relating to the situation in Northern Ireland that reached Strasbourg confirmed that the UK was in a state of emergency that qualified for a permissible derogation at this time, it seems unbelievable that we have maintained this status throughout. The actions of Al-Qaeda may well once again present such a serious threat, however it is known that this is not likely to diminish for some years. We therefore think that the derogation should be construed as temporary measures until the UK government formulates comprehensive and effective terrorism laws that do not involve a derogation and hope to see some evidence of this in the very near future.

On the Use of Intercepts as Evidence

On the ban on the use of intercepted communications in court, the Newton Committee notes that "[o]ne way of making it possible to prosecute in more cases would be to remove the UK's self-imposed blanket ban on the use of intercepted communications in court." The Government's concern, given during the debates on the Regulation of Investigatory Powers Act 2000 on allowing the use in evidence, is that this would reveal the authorities' capabilities, and thus prompting criminals to take more effective evasive action.

There is, however, no ban on the use of foreign intercepts obtained in accordance with foreign laws. Also, bugged communications or the product of surveillance or eavesdropping, even if not authorised and if they are an interference with privacy, are allowed as evidence. Nor is there a bar on foreign courts using British intercept evidence.

| | |
|-----------------------|---|
| Newton Recommendation | Call for a relaxing of the ban. The Committee is careful to note that this would not require the prosecution to use the evidence. Also, they can see the case for changing the rules governing the disclosure of evidence so that the prosecution would not be obliged to disclose intercept evidence, or even its existence, unless they chose to rely on it. "This would need to be done with care to minimize the risk of miscarriages of justice", but those "risks should not be greater than under the present system where the prosecution is forbidden from disclosing intercepted communications, even if they are exculpatory." |
| Home Office Response | Subject to review. "It is important to ensure that any decision on whether or not to change the law is based on a rigorous assessment of the likely impact (e.g. in securing more prosecutions) and clear evidence that the benefits of doing so clearly outweigh the risks." |

In relation to detention, if the removal of such a ban in cases of suspected terrorism would enable trials to proceed, the inference currently being that it would, then it is a topic that requires immediate attention. If the authorities are using such evidence as a main or sole basis for the detention of that individual, it seems unnecessary to not bring such evidence to court to allow a trial to proceed. The Home Office in its Discussion Paper merely mentions the fact that the ban is currently under review but contributes nothing by way of opinion as to what they would hope the outcome of this review will be or whether a removal of the ban could induce more trials which they are currently claiming cannot proceed.

Privacy International opposes the use of intercepts as evidence in general cases, however. Such evidence can be interpreted by a jury in an irrational and emotive way -- similar to the so-called infallible evidence of DNA. If such evidence was to be introduced then defence lawyers would need to have advance notice to prepare a possible defence or response. This could be presented in chambers to a judge who can rule according to the circumstances of each case whether it should be admitted. Full disclosure by law enforcement authorities of the circumstances of the interception should also be made, including the validity of the devices used and the legality of the results. Law enforcement authorities should not be permitted to selectively disclose wiretap evidence (i.e. by selecting the thirty seconds that suit them).

We therefore see this as an opportunity to open up the opaque area of communications surveillance, by allowing the defendant's attorneys to see this information and to see how widely they cast the net when they do interceptions. But we don't accept that transcripts of conversations are valid evidence in all cases. If the material in an intercept was valid then police should surely be able to pursue it to discover evidence. There is a risk that convictions may be pursued just on the basis of implied intent.

We also find it quite unacceptable that foreign evidence may be used even when it is collected with a lack of legal rigour.

On Using Surveillance Instead of Detention

| | |
|-----------------------|--|
| Newton Recommendation | Argues that surveillance can help spot indications of terrorists forming their organizations, developing capabilities, gathering information on potential targets. "It can help to identify terrorists re-entering the country after training, uncover safe houses, identify arming and financing channels and help to establish networks of informants. The use of surveillance does, of course, have adverse human rights implications, as well as lacking the certainty of detention." They see the use of new technology to allow for better surveillance, "although the use of more intrusive techniques requires adequate safeguards." Calls on the Government to examine the more intensive use of surveillance. "We have in mind not simply the marking of particular individuals or groups, but also training, the use of technology and better liaison between different agencies at ports of entry." |
|-----------------------|--|

| | |
|----------------------|---|
| Home Office Response | <p>Surveillance cannot offer the same levels of protection as detention. Argue that surveillance is resource intensive. Contend that the Home Office has increased funding and support for law enforcement agencies already.</p> <p>"These developments are part of a wider picture and we have already announced proposals for Serious and Organised Crime Agency. The Government is also working to develop better co-operation between HM Customs and Excise, the Police and the Immigration Service. All have a role to play in safeguarding our borders, defending us against organised crime, financial fraud and terrorism."</p> |
|----------------------|---|

We appreciate that even with the addition of separate terrorism laws, it may not be conceivable from the Government's point of view to bring all suspected terrorists to trial where undermining an ongoing source of information is concerned. In such circumstances, surveillance as opposed to detention presents an option, provided that due process remains the priority and it has been objectively ascertained that a trial cannot proceed (potentially by a security cleared judge).

Whilst the Home Office comments at paragraph 40 that "effective surveillance is resource intensive", the Home Secretary also reminds us in the foreword that 17 individuals have been detained under Part IV powers. We would like to suggest that in relation to such a small number of individuals, the costs of intensive surveillance are not disproportionate to the importance of maintaining a person's liberty, even if this may only mean not being held in a high security prison.

The use of such invasive methods should not be used arbitrarily, however and, while as mentioned it would only be in circumstances where a trial cannot commence, fundamental principles such as suspicion beyond reasonable doubt should be applied. We are concerned with these recommendations and the response. We would welcome a more in-depth discussion regarding policy changes in this arena.

Privacy International generally supports the use of surveillance when used as a genuine alternative means of detention. We would not like to see this used, however, in more general situations as an alternative form of punishment for crimes that would not otherwise have resulted in detention.

On Other Restrictions

Along with detention, restrictions of access to communications and other facilities are also considered.

| | |
|-----------------------|---|
| Newton Recommendation | Recommend the use of restrictions on the freedom of movement, and the ability of suspects to use financial services, communications or associate freely, arguing that such an approach is used in France and Sweden. |
| Home Office Response | "The Government does not believe that tagging or the other measures suggested offer sufficient security to address the threat posed by international terrorists. Modern technology such as pay as you go mobiles, easy access to computers and other communications technology mean that tagging by itself would not prevent these individuals from involvement in terrorism and the Government can not guarantee the success of such an approach." |

We do agree with the government that it would be very difficult to prevent access to communications devices, nor would we want to see extended surveillance of communications devices.

On Deportation Agreements

| | |
|-----------------------|---|
| Newton Recommendation | <p>In arguing that deportation of detainees is possible, the Committee says</p> <p>"In cases where deportation is considered the only possible approach — and we have considerable reservations about it as a way of dealing with suspected international terrorists — we have seen no evidence that it would be illegal for the Government to detain the deportee while taking active steps in good faith to reach an understanding with the destination government to ensure that the deportee's human rights were not violated on his return. This is what some other countries seem to have been able to do, at least in some cases.</p> <p>[...] We are aware that there has been at least one case where the judges concluded that the assurances that the UK Government had obtained from the destination government did not, in the light of other evidence, provide a sufficient degree of reassurance about the safety of the deportee on his return. Such judgements do not, however, invalidate the principle of the approach."</p> |
| Home Office Response | <p>Case law in deportation is 'quite clear'. For detention to be lawful there has to be a reasonable prospect of removal within a reasonable period. Without derogation, (and section 23 of ATCS), 'we would have no option but to release if an acceptable undertaking could not be obtained within a reasonable period.'</p> <p>The Government acknowledges that undertakings are not always achievable, possibly because destination governments decline to enter such negotiations, or they are delayed, or if the terms are insufficient.</p> |

We are sympathetic to the Government claims of the problems of negotiations. We are reminded of some of the legal problems and human rights abuses that have arisen under the claims of 'international co-operation', most recently in the case of Mohammed Arar in Canada. Arar was sent by the U.S. Government to Jordan and then sent to Syria where he was tortured. Such 'extraordinary rendition' would be illegal under UK law, and attempts to increase deportation are likely to give rise to similar cases. We need greater clarity in cases of deportation, not backroom agreements that are not worth the paper they are written on.

On Race and Religious Hate Crimes

| | |
|-----------------------|---|
| Newton Recommendation | <p>"Terrorism legislation agreed on an emergency timetable was not the appropriate context for measures that raised important and contentious matters of principle and expediency that merited careful deliberation". In testimonies to the Committee, some complained that the sections were a 'sop to the Muslim communities', even though its repeal, in isolation, would be undesirable, but also that the law provides serious difficulties for prosecutors.</p> <p>"[A]ny such measure has no place in terrorism and security legislation".</p> |
| Home Office Response | <p>The government will consider whether the system can be improved, but has not identified any early opportunities for reform.</p> |

We do not believe that criminal sanction should be overly affected by motivation, or that these measures belong in terrorism law.

We fail to see the substantive difference between the aggravation element of a racially motivated attack, which has passed scrutiny to become part of our criminal law thus allowing different penalties, and the feasibility of a similar aggravation element for a criminal offence with a proven terrorist link, which could also allow penalties of differing severity.

On Advanced Passenger Data

| | |
|-----------------------|--|
| Newton Recommendation | 'The Committee believes that this information is valuable. They note that carriers have cited practical, data protection and financial barriers to providing the information, "but it would appear that these objections have not prevented the provision of similar information to U.S. authorities." Call for more consultation with the carriers. |
| Home Office Response | 'The Government has already carried out extensive consultation with the carriers on this matter. Care has been taken to 'balance' the need of law enforcement agencies and resource implications on the carriers. As an example, for internal journeys in the UK, carriers only have to provide information on passengers when requested as part of an ongoing Police investigation.' "The Government regards this as a key power in tracking the movement of terrorists." |

The change in the law was significant: previously the Terrorism Act 2000 applied only to ships/crafts arriving from Ireland and Northern Ireland. The law was changed to apply to any arrival from within and outside of the United Kingdom.

This power appears to be on a case by case basis, and specific, although the SI seems to include more information than is usually disclosed, including 'place of birth' and 'nationality' which is arguably unnecessary for national flights.

We disagree with the Newton Committee's assessment that the data protection, financial, and practical barriers to the provision of this information is not prohibiting the transfer to the U.S. authorities. Passenger manifests to the U.S. is very limited in nature, meanwhile the passenger-name records are much more complex.

We are quite concerned regarding the use of this information for non-terrorism purposes. Much controversy has arisen in other countries regarding the collection and use of this data for purposes other than provision of air security, particularly in combating terrorism. We oppose its use for internal flights, in particular. A similar law in Canada went through three iterations; here it is held on ambiguous grounds in primary law and SIs.

The systematic transfer of this data does have data protection conflicts because any transfer, while lawful, must be specific and proportionate and its purposes and uses clearly laid out. Neither the laws nor SIs involved do this sufficiently.

Clear statutory grounds for these transfers are required. And we must ensure it is only used for combating terrorism. We must ensure that this data is not used for new criminal purposes without sufficient legislative mandate.

On Police Powers to Force Identification

Under Part 10, the police may take fingerprints using reasonable force in order to identify an individual under detention, and take photographs. All of these photos and fingerprints may be retained for the purposes of the prevention and detection of crime.

Previously, the Police and Criminal Evidence Act applied fingerprint retention to cases where persons were convicted or charged or cautioned for a recordable offence or where there were reasonable grounds to suspect their involvement in a criminal offence and fingerprints would tend to confirm or disprove it.

| | |
|-----------------------|--|
| Newton Recommendation | <p>Most of the uses of Part 10 powers have not been related to counter-terrorism.</p> <p>The use of these powers has not been systematically recorded. "Their usefulness in relation to other crimes is more difficult to assess."</p> <p>"Apparently the Government in 2001 resisted limiting the use of these powers to terrorist cases on grounds that even where there are initially no grounds to suspect involvement in terrorism, such an identity check might establish that one exists. However, amongst the cases that were reported to us, none of these uses resulted in the identification of terrorists who had been in custody for other reasons; the majority involved individuals who had been detained under the Terrorism Act in any case."</p> <p>The Committee goes on to say that the retention of fingerprints was established in the Criminal Justice and Police Act 2001 (and since extended in the Criminal Justice Act 2003, when it was extended to ALL those who have been <i>arrested</i> rather than having to be charged as under the 2001 Act). "It was controversial, and ought not to have been extended in emergency legislation."</p> <p>Recommends that "the privacy of innocent citizens ... should be protected." The Committee calls for amendments to permit retention only in circumstances where the subject is charged with an offence (returning to circumstances in which they can be retained under the 2001 Act), or where appropriate authorisation is given that they are of ongoing importance in a terrorist investigation.</p> |
| Home Office Response | <p>When the identity of someone is not known, the police may not establish until investigations are underway whether or not the person has links with terrorism.</p> <p>"There has, thankfully been a low level of terrorist incidents, so the majority of uses have been in cases where police have sought to ascertain identity for non-terrorism purposes, as these powers amend PACE identification provisions generally. However, where used in terrorist situations the powers have proven important and justified by their counter-terrorism benefits."</p> <p>"(...) Nevertheless, the police have welcomed the new powers and the level and scope of there (sic) use to date suggests the (sic) have proved appropriate and useable."</p> <p>" (...) Law abiding citizens have nothing to fear from having this information retained. Retention of fingerprints in these circumstances is considered to be proportionate and of benefit to the interests of society for the purposes of prevention and detection of crime."</p> <p>Due to changes in the CJA 2003, "It would not be appropriate to have lesser powers for counter terrorism than those already in place for routine criminal investigation."</p> |

The response from the Home Office appears to use circular reasoning. It may be summarised as follows: 'When arrested for something else, it would be helpful to know if person is wanted for terrorism. As there has been little terrorism, this power is often used for non-terrorism purposes. Police are happy with these powers. Law abiding individuals have nothing to fear. So we can use these powers across the board. And the new laws let us use this power for any situation, so now going back and changing ATCS 2001 would mean that we can't use this power for terrorism cases.'

The Committee calls for a judgement decision on whether someone's fingerprints may be of use in a terrorist investigation, which is a remarkably low barrier, but is at least a test of specificity. The Home Office appears intent on keeping whatever powers it was able to get in times of duress. This is absurd.

The privacy of all those who are arrested and those who fall under immigration law are affected by the decision to retain fingerprints; and thus not just criminals and terrorists. This must be limited to specific cases where people are charged and found guilty. While the Law Lords decided the proportionality of the retention of fingerprints and DNA samples on grounds that

- (i) the fingerprints and samples are kept only for the limited purpose of the detection, investigation, and prosecution of crime;
- (ii) the fingerprints and samples are not of any use without a comparator fingerprint or sample from the crime scene;
- (iii) the fingerprints and samples will not be made public;
- (iv) a person is not identifiable to the untutored eye simply from the profile on the database, any interference represented by the retention being minimal;
- (v) and, on the other hand, the resultant expansion of the database by the retention confers enormous advantages in the fight against

serious crime. Cumulatively these factors suggest that the retention of fingerprints and samples is not disproportionate in effect.

we agree with the dissenting opinion on the issue of retention from Baroness Hale

Storing information almost inevitably involves someone else knowing it. It is an interference with privacy for someone to know or have access to private information even if they make no other use of it. The mere fact that someone has read my private correspondence or seen my bank accounts is an interference with my privacy even if that person tells no one else what he has seen. That is why access to private information such as that contained in medical records has to be carefully controlled. The fact that only a few people can understand the information does not affect the principle, although it may affect the justification.

We would like to remind the Home Office of the problem of inaccurate matches of fingerprint data. The case of Brandon Mayfield is particularly interesting, considering that the experts in the Department of Justice in the U.S. declared with certainty that his fingerprints were found on items related to the Madrid Bombings, despite this not being the case. He was, in turn, detained for two weeks due to this error. The appearance of 'conclusiveness' of fingerprints is worrying and we find that travesties of justice have arisen when fingerprints are inappropriately used and analyzed.

As more and more fingerprints are collected, the error rates are likely to increase significantly, and we therefore recommend that the Government act prudently and limit its collection merely to what is strictly necessary. Otherwise errors will increase, and problems will arise. Those with nothing to hide will have much to fear.

In the face of the Newton Committee recommendations, and the clear ethical problems that arise from the Law Lords decisions, we appeal to the Home Office to restrict this over-broad power that will affect innocent individuals, that contributes to a larger and larger database and sharing of information across borders.

On Identity Theft

| | |
|-----------------------|--|
| Newton Recommendation | Concerned about the ability of individuals to use fake documents. |
| Home Office Response | All powers are effective and proportionate. ID cards will solve this, 'which gives them a secure but easy way of demonstrating their right to be resident and their entitlement to public services.' |

We oppose this mode of thought, this policy, and this reasoning, as we have stated repeatedly elsewhere (see <http://www.privacyinternational.org/ukidcards>). Securing documents is one activity; creating back-end databases of all citizens and residents (except for EU nationals) is another proposal altogether. It is disappointing that after many statements from the Home Secretary admitting that ID cards will have little effect on terrorism, the Home Office continues to claim that biometrics ID cards and national registers will 'provide better protection from terrorists'.

It is also important to note that the fake documents leading to September 11 2001 were not as remarkable as the lack of awareness and verification of the fact that some of these individuals were wanted terrorists. Visas were issued for these individuals despite their status as terrorists. The mass identification of law abiding citizens is not the solution to the failures of government projects and departmental policies.

On Fingerprinting and Immigration Policy

In Part 4 section 36, the ATCS 2001 removed the requirement that immigration authorities should destroy fingerprints once they had met their purpose, for instance, once the individual concerned had been given indefinite leave to remain, or their identity as a UK or Commonwealth citizen with right to abode had been established. As a result, all fingerprints taken for immigration purposes can now be retained for ten years, on the grounds that they might be useful to a criminal investigation at a later stage. This would also apply to UK citizens.

| | |
|-----------------------|---|
| Newton Recommendation | The Joint Committee on Human Rights commented that they were not persuaded that this is a proportionate, and could stigmatize immigrants, and has no clear connection with terrorism or security. Calls for the previous position on retention to be re-instated, except where appropriate authorisation is given that the fingerprints are of significance in an ongoing terrorist investigation. |
| Home Office Response | The goal of this section was to prevent people from obtaining a second identity. "Fingerprints are the only established way beyond doubt of linking a person to a previous identity". Retention makes it harder to create a false identity by making a further asylum application. It also prevents other crimes, and "has in particular prevented abuse of the asylum process by preventing those granted asylum reapplying for asylum in another identity." |

This power has nothing to do with terrorism, and as argued above, retention of this data is unnecessary, and the powers are thus unnecessary, particularly in an emergency legislation.

On Removing Disguises

The Act amended the Criminal Justice and Public Order Act 1994 relaxing controls on the powers by reducing the rank of the police officer who authorises the removal of the disguise, and the circumstances in which the powers might be activated were broadened from incidents involving "serious violence" are likely to occur to those where "offences" in general are likely to occur.

| | |
|-----------------------|---|
| Newton Recommendation | Voices concerns about the absence of safeguards against abuse. Also concerned about the double extension of the power. Recommends that previous limits be restored, although a more strictly defined power may also be retained for those cases where a senior police officer believes that this measure is necessary in response to a specific terrorist threat. |
| Home Office Response | Face coverings and outbreaks of public disorder are increasingly widespread. "There may be links between demonstrations where face coverings are worn and terrorist activity. These may not always be obvious or necessarily based on the declared objectives of the protest. However, in strictly defined circumstances the police should be able to require the removal of disguises and thus prevent people moving around in public places with their identity concealed." "Government believes that restricting this power would constrain the police's ability to identify those who seek to hide their identity for terrorism and other criminal purposes." |

We agree with the Newton Committee that there must be a specific terrorist threat throughout the use of this power, to ensure that it is not applied generally to any public protest. As we have already seen, the Court of Appeals has permitted the arbitrary use of stop and search powers enabled by a senior police officer in the case of terrorism. It is our opinion that the Court of Appeals decided wrongly, that the right of free expression is important to uphold, even in these times of concern regarding terrorism.

The decision by the Court of Appeals hinged on the link with terrorism. It is unlikely that the Courts will uphold this law that applies so broadly, and so we advise that it be changed.

On Traffic Data Retention

| | |
|------------------------------|---|
| <p>Newton Recommendation</p> | <p>Contends that traffic data allows investigators to identify suspects, examine their contacts, establish relationships between conspirators and place them in a specific location at a certain time.</p> <p>The 'disparity of purpose', where data retained for national security purposes but accessed for other purposes, "seems to us to be a fundamental difficulty with the framing of these provisions."</p> <p>The Committee notes that:</p> <p style="padding-left: 40px;">"we believe it would be beneficial both for users and subjects of the data if retention and access were based on a coherent statutory framework: the Home Office have indicated that work in the EU context may, eventually, provide the basis of such a framework."</p> <p style="padding-left: 40px;">"(...) We can see the case in principle for requiring communications data to be retained for a minimum period (which would vary with the type of data) for a defined range of public interest purposes such as helping in the prevention and detection of terrorism and other serious crime. These provisions should, therefore, be part of mainstream legislation and not special terrorism legislation."</p> <p>"(...) From what we have seen, the costs of retention do not appear to be excessive."</p> <p>States that there are obvious privacy risks, with potential for abuse.</p> <p style="padding-left: 40px;">"the Government should accept the logic of the results of its consultation and replace Part 11 with a mainstream communications data retention regime which limits in primary legislation the longest retention period which the Government can impose to one year. This approach seems to have been adopted in several other European countries. It would permit data which is of potential use in safeguarding national security to be retained. Access to the data must, however, be subject to strict regulation, and that regulation must be properly enforced."</p> <p>Recommend oversight by the Information Commissioner.</p> <p>Call for data preservation powers.</p> |
| <p>Home Office Response</p> | <p>"The Government would ... like to see data retained for the purpose of fighting crime generally."</p> <p style="padding-left: 40px;">"The Government does not particularly see the necessity for putting data retention periods in primary legislation rather than secondary legislation." Changes in technology and the industry are quick, and the Government "therefore requires a relatively speedy process in order to make additions to the types of data to be retained and the periods of time for which they are retained as and when it is deemed necessary."</p> <p>The Government has no plans to put data preservation on a formal footing in the same piece of legislation as data retention.</p> |

We disagree fundamentally with any perception that retention is legal, useful, fair, and cost-effective.

Data retention is for intelligence purposes. It does not tell you who did something wrong. It may be used to help investigate crimes, but it is not conclusive. Meanwhile it is costly, unnecessary, and in contravention to human rights principles. The grounds upon which the Committee believed that retention was a valid practice are false. We are perplexed that a Committee that has done so much to review the other powers in this Act seems to have failed to give adequate scrutiny to this most dangerous section of the law that applies to all people, and not just terrorists and criminals.

Meanwhile this data is highly sensitive personal information. As we have argued previously, traffic data is capable of disclosing highly personal information, and at times, a biography of an individual's life. As such even the Council of Europe calls for regulating its preservation and access because

"The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures."

Even as the link between the individual and the traffic data is tenuous, the fact that all of this information is collected and accessed on any number of grounds is highly problematic.

If the Information Commissioner was to oversee this entire process, the Information Commissioner would need greater powers, and there would need to be better oversight and authorisation and reporting regimes on access to traffic data. In this sense, we agree with the Government that we need a Commissioner who will initiate action, not a complaint-based, responsive, regulator. However we have found the Interception Commissioner to be wholly inadequate in his role and thus greater oversight through a better positioned and more rigorous office would be ideal, at the very least, to oversee access.

We do not accept the argument that secondary legislation is ideal for data retention periods. This is exactly the situation that arose in November 2003. Rarely has secondary legislation been refused by Parliament. With the changes in technologies and increased awareness of the powers granted to the Government through the police of retention, it must be revisited in primary legislation every time a new form of technology is added, and a new period of retention is implemented. It is undemocratic to do otherwise. We call for clear deliberation on any collection, retention, and access scheme, not a rushed process due to technological change.

Accepting a voluntary regime is merely a stepping stone to a pan-European regime for retention. We find it disingenuous that the Home Office is implementing a voluntary regime even as it is pushing for a mandatory regime in Europe. This policy laundering is not going unnoticed, and it is insulting to the democratic process.

We call for a complete revisit of data retention in primary legislation, away from the false premise of a link to combating terrorism, to give the policy a chance to stand on its merits.

On Secondary Legislation

Part 13 of the ATCS 2001 allows certain EU obligations relating to police and judicial co-operation in criminal matters to be transposed into UK legislation by secondary, rather than primary legislation.

| | |
|-----------------------|---|
| Newton Recommendation | <p>The case for secondary legislation in police and judicial cooperation ('third pillar') is much weaker than in 'first pillar' (e.g. single market) because</p> <ul style="list-style-type: none"> a. issues of liberty and accountability tend to arise in legislation on policing and the judicial process to a greater extent; b. unlike, for example, the single market programme, the volume of "third pillar" obligations is not high; c. not all such obligations require legislation: <ul style="list-style-type: none"> i. UK legislation is often fully or wholly in compliance with them; ii. Some obligations require administrative and not legislative action. d. implementation deadlines have not been unmanageably tight; e. there is a greater frequency of primary legislation suitable for enacting third pillar legislation (e.g., criminal justice bills). |
| Home Office Response | None. |

We are surprised to see that the Government did not comment on this. We could not agree more with the Newton Committee on this matter, and we see it as linked with the issue of data retention, as the UK is leading the initiative at the EU under the third pillar. Secondary legislation is the means through which policy laundering is implemented.

On Consequential and Supplementary Provisions

Supplemental and consequential changes to law may be made, through negative resolution procedure, to amend legislation.

On 'negative resolution',

"they do not need to be approved by an affirmative vote in Parliament at all. With certain very limited exceptions, delegated legislation subject to the affirmative or the negative procedure may not be amended by either House of Parliament. Instruments exercising delegated powers are affirmed, or made the subject of a "prayer" (a motion to annul) as a whole. In the House of Commons, the Government cannot be forced to find time for a debate on a motion to annul or to revoke an instrument subject to negative resolution, either on the floor of the House or in Committee. If such an instrument were to be referred to a Standing Committee, the motion for debate would be "that the Committee has considered the instrument": even if such a motion were defeated in Committee, there would be no legal or procedural consequences, and the Government would not be obliged to put the substantive motion to the House. The House of Lords Committee on Delegated Powers takes the view that all such instruments should be subject to affirmative resolution procedure: Session 2002-3, 3rd Report."

| | |
|-----------------------|---|
| Newton Recommendation | <p>It is accepted that 'Henry VIII' powers are sometimes appropriate, to allow the Government to make technical amendments to complex Acts of Parliament through subordinate legislation.</p> <p>But the powers here are amongst the broadest of their kind in that:</p> <ol style="list-style-type: none"> a. they provide for "supplemental", as well as merely "consequential" amendments; b. they are subject only to negative resolution procedure, contrary to the explanation given in the Home Office memorandum, and; c. they include a power to amend legislation passed before the 2001 Act. <p>This power, while not totally unprecedented, is "inappropriate and unwelcome, in an Act where so many provisions were known to be controversial, raising a number of civil liberties issues. The powers of amendment set out in Section 124 are particularly unwelcome in emergency legislation of this kind, and they should be repealed."</p> |
| Home Office Response | <p>"Disagree. The Government believes that this power allows the Government to react quickly to changing circumstances that are a feature of many of the areas covered in the Act. It is correct that terrorism legislation is placed on a permanent footing and that powers contained within it allow us to respond flexibly to any changes in threat."</p> |

This is a half-hearted response from the Government. We agree with the Newton Committee, and see this as a practice that is consistent with other practices by the Government to minimize scrutiny, deliberation, and debate. It is inimical to the idea of an Open Society, and should be abandoned.

Privacy International, August 2004.