



**Liberty's response to the National
Policing Improvement Agency Equality
& Privacy Impact Assessments: MIDAS
& Lantern Mobile Fingerprinting
Projects**

September 2009

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at

<http://www.liberty-human-rights.org.uk/publications/1-policy-papers/index.shtml>

Contact

Isabella Sankey

Director of Policy

Direct Line 020 7378 5254

Email: bellas@liberty-human-rights.org.uk

Anita Coles

Policy Officer

Direct Line: 020 7378 3659

Email: anitac@liberty-human-rights.org.uk

Introduction

1. In 2006 police forces in a number of regions started the Lantern mobile Fingerprinting Project. This project uses mobile technology to fingerprint people away from the police station. The project was created as a result of a request by the Automatic Number Plate Recognition (ANPR) Steering Group who wanted police officers to be able to identify drivers on the spot, rather than taking them to the police station when an officer doubted the identity of a driver.¹ We understand that mobile fingerprinting pilots and field trials are currently underway in 28 police forces, with bigger forces such as the Metropolitan and Manchester police using a large number of devices.

2. In June 2009, the National Policing Improvement Agency ('NPIA') published Equality and Privacy Impact Assessments on the use of the Lantern technology which includes proposals for the future use of the devices. This is an unusual consultative exercise in that it considers police operational practice and procedures that have been developed by the police with little parliamentary oversight. We welcome the opportunity to respond to the consultative impact assessments. As we outline below we have a number of concerns in relation to the use of this technology and the lack of appropriate oversight.

Legislative Framework

3. The *Police and Criminal Evidence Act 1984 (PACE)*² governs the taking of fingerprints. Under PACE, the police must gain a person's consent before taking their fingerprints. However, there are circumstances where the police can take fingerprints without consent. Section 61 of PACE provides that the police can take fingerprints without consent from a person who has been arrested or charged with a recordable offence³ and who has not already had his or her fingerprints taken in the course of the investigation of the offence by the police;⁴ or if a person has been convicted of a recordable offence, cautioned for an admitted recordable offence or has been warned or reprimanded under section 65 of the *Crime and Disorder Act 1998* for a

¹ See MIDAS & lantern Equality Impact Assessment Consultation Paper, pg 5.

² See sections 27, 61, 63A and 64 of PACE and the Identification Code.

³ The definition of a recordable offence is contained in section 118 of PACE and the *National Police Records (Recordable Offences) Regulations 2000*. A recordable offence is defined as being any offence punishable by imprisonment as well as 68 other named offences.

⁴ See section 61(3) (b) and (4) of PACE.

recordable offence.⁵ Every person arrested for a recordable offence has their fingerprints entered onto the National Fingerprint Database. Under current law, where a person has been arrested, charged or informed he or she will be reported for a recordable offence and fingerprints may be checked against other fingerprints held by or on behalf of a police force.⁶ PACE currently provides that fingerprints may be retained after they have fulfilled the purpose for which they were taken.⁷ Where fingerprints are taken from a person who is not suspected of committing the offence in question, they must be destroyed as soon as they have served their purpose.⁸

4. The *Serious Organised Crime and Police Act 2005* (SOCPA), section 117, introduced new sub-sections into section 61 of PACE, allowing a constable to take a person's fingerprints without consent if the constable reasonably suspects that a person has committed or attempted to commit an offence, and the name of the person is unknown and cannot be easily ascertained by the constable, or the constable has reasonable grounds for doubting whether a name given by the person is his or her real name.⁹ As the explanatory notes to the Act, when going through Parliament, made clear, section 117 was enacted specifically with mobile fingerprinting technology in mind. However, these sections have not yet been brought into force.¹⁰ So as the current law stands, there is nothing that gives police officers the power to take a person's fingerprints in such circumstances.

Impact Assessments and Consultation

5. . Before commenting in detail on the current and potential use of mobile fingerprinting it is important to note that Liberty does not take issue with the use of mobile fingerprint technology in itself.¹¹ As noted above, fingerprints can only be taken without consent in limited circumstances. With this in mind, technology that

⁵ See section 61 6 of PACE.

⁶ See section 63A (1) of PACE.

⁷ See section 64 of PACE.

⁸ See section 64(3) of PACE.

⁹ See section 61 (6A) – (6C) of PACE.

¹⁰ Liberty understands that there is some confusion as to the meaning of this section within police forces. It is clear that, once in force, section 61(6B) must be satisfied before fingerprints can be taken without consent. The test goes beyond just suspecting the individual of a crime. The subsection requires that fingerprints can only be taken without consent if the officer does not know the person's name and their name cannot be reasonably ascertained (i.e. by asking for identification etc) or alternatively, the officer has reasonable grounds to doubt the name given to them. Only if one of these two conditions is satisfied can an officer use mobile fingerprinting technology on a person who has not been arrested.

¹¹ See *The Guardian*, 'Police will use new device to take fingerprints in the street', 27 October 2008 <http://www.guardian.co.uk/politics/2008/oct/27/project-midas-fingerprint-scanner-liberty>.

allows a person's fingerprints to be taken on the spot, where that person might otherwise be arrested and taken to a police station, seems to be both proportionate and beneficial. Additionally, we have always understood that while mobile fingerprinting technology allows police officers to identify a member of the public using images of their fingerprints, it does not allow for the retention of any fingerprint images. Instead, the fingerprints are checked against the centrally stored database but no record of the fingerprint is kept. However as we note below, we are concerned by an indication in the Privacy Impact Assessment Background Paper that this may no longer be the case.

'Consent based' fingerprint identification

6. While we do not take issue with the technology per se, we do nevertheless have concerns about a number of related issues raised in this consultation. First, while the consultation states that the introduction of mobile identification through Lantern will not extend the range of circumstances in which an officer can seek to establish identity,¹² we are concerned that the new found ease of fingerprint identification could have the effect of usurping the grounds for which fingerprint identification is permitted in legislation. Indeed we are concerned that this has already happened in practice with the introduction of purported 'consent based' fingerprinting that does not allow for truly informed consent in practice. We understand that the current pilot schemes are premised on individuals giving written consent to fingerprint identification when asked by a police officer. The consultation makes clear that because the relevant sections of PACE are not yet in force, officers currently seeking to ascertain identity while using Lantern need to obtain a person's consent before taking their fingerprints.¹³ However, when a uniformed officer asks an individual to provide a fingerprint, the likelihood is that the individual asked will assume they are either suspected of something or that they have some kind of obligation to provide identification. Even if a police officer expressly says that there is no obligation, there is still a good chance that an individual may feel intimidated and compelled to provide a fingerprint. This will especially be the case if the individual believes that they may be taken to the police station if they do not provide a fingerprint. It is unlikely, for instance, that people would provide their fingerprints to another private individual if simply asked to do so, and equally unlikely that an

¹² See MIDAS & Lantern Equality Impact Assessment Consultation Paper, pg 8.

¹³ See MIDAS & Lantern Equality Impact Assessment Consultation Paper, pg 8.

individual would willingly accompany an officer to the police station to have their fingerprints taken when they have been told there is no obligation to do so. It is crucial that the convenience of having technology that allows fingerprints to be taken on the spot, does not override the fundamental principle that there is no general obligation to provide identification when asked by an agent of the State.

7. Legislation has already provided police with the power to take a person's fingerprints without consent when an officer reasonably suspects that an individual has committed or attempted to commit an offence, and is unable to identify the person. Although the Government has not yet brought these provisions into force, it was clearly Parliament's intention when legislating that these powers only be used in the circumstances prescribed. Section 61(6A) – (6C) only allows the police to take fingerprints where the name of the person is unknown and cannot be easily ascertained by the constable, or the constable has reasonable grounds for doubting whether a name given by the person as his or her name is their real name. Given that Parliament has not legislated for 'consent-based' fingerprinting and given the very real difficulties in obtaining real and informed consent in such circumstances Liberty does not believe that a purported 'consent-based' approach to fingerprinting is a viable option for police. We are instead concerned at its back-door introduction which appears to be motivated in part by the fact that section 61 of PACE has yet to be brought into force. If the police are not restricting the use of their powers to those expressly granted by Parliament, then they risk acquiring de facto powers by virtue of their professional position.

8. Of further concern is the potential for the supposed 'consent-based' approach to become a routine method of police identification. We understand that those piloting the mobile fingerprinting devices currently claim only to seek identification when an individual is suspected of an offence. This appears to be an attempt to read across the PACE provisions on mobile fingerprinting (without consent) that are not yet in force. However Liberty has been made aware, anecdotally, of the routine use of mobile fingerprinting devices for vehicle users. This reveals one of the key problems with the so called 'consent-based' approach to mobile fingerprinting: namely that it is a doctrine created by police that hugely expands their powers in practice. Currently the greatest restraint on its use – that it is only used on those suspected of an offence – is self-imposed.

9. Liberty is also concerned that the availability of mobile fingerprinting devices shouldn't replace other traditional forms of establishing identity. Methods of identification exist on a sliding scale – some more intrusive than others. Liberty has always acknowledged the usefulness of fingerprint and DNA profiles in detecting and preventing crime. This does not mean however that police should have blanket powers and tools to request fingerprint identification whenever it suits. Less intrusive mechanisms of identification – such as asking somebody their name or for some other proof of identity – should always come first. In circumstances where identification can be lawfully¹⁴ sought, an individual should be asked to identify themselves and then only asked for fingerprint identification if there is a suspicion that the person has given false details.

10. We also have real doubts about the effectiveness of immediately fingerprinting a person before asking for alternative forms of identification. The consultation document appears to make the false assumption that fingerprint checks will always reveal a person's identity. Fingerprint checks will only help to identify a person where they are already on the fingerprint database because they have been either arrested or convicted of a recordable offence. The vast majority are not on the database and their identity will therefore not be revealed through mobile fingerprinting. A linked concern is that an automatic recourse to mobile fingerprinting will, again via the back door, become a means by which police officers confirm suspicions about individuals. Although the database stores the fingerprints of thousands of innocent people, those on the database are undeniably stigmatised. We are concerned that premature recourse to fingerprinting, followed by positive matches, will in practice confirm suspicions among police officers that a further offence has been committed.

Data Retention

11. The Privacy Impact Assessment Background Paper (PIA) raises several important privacy issues. The MIDAS & LANTERN Equality Impact Assessment indicates that the fingerprint images obtained through mobile fingerprinting will not be retained.¹⁵ However, page 16 of the PIA states:

¹⁴ Using powers under PACE which should be brought into force to allow this.

¹⁵ At page 4: "In considering [whether the service is proportional and appropriate] it may be useful to recognise that the capability; does not retain any fingerprint images"

One area of concern is whether and for how long images of fingerprints captured by MIDAS will be stored, whether this will lead to an ever expanding central fingerprint database even where no match has been detected... we must consider whether the storing of fingerprint images of an individual and any matched data items such as name, date of birth and gender infringes their privacy. Short-term retention of matched data items may be necessary for audit purposes.

This is confusing and seemingly inconsistent. Following the European Court of Human Rights (ECtHR) judgment in *S and Marper v UK*¹⁶ the proposal in the PIA is also likely to be unlawful. In that case, in a strongly worded and unanimous judgment, the Court accepted that the retention of DNA information and fingerprints pursues the legitimate purpose of crime detection and prevention, but went on to say that the blanket indefinite retention of such material is not necessary in a democratic society as it fails to strike a fair balance between competing public and private interests and is a disproportionate interference with the right to privacy.¹⁷ The National Fingerprint Database as currently constituted was found to be unlawful. As a result, the Government is currently considering how the fingerprint retention regime must be reformed in order to comply with the Strasbourg judgment. It is curious, if not alarming then, that at the same time, the PIA seem to be considering retaining fingerprints and additional information of those who have not even been arrested, let alone charged or convicted. This would hugely expand the reach of the database and doubtlessly put the UK further in breach of human rights law. It is essential that fingerprints should not be retained longer than is necessary to secure an identification match.

Database duplication

12. The PIA states that it has not yet been decided whether fingerprint matching will be carried out by using the existing fingerprint database or whether a separate matching database will be created. As far as we are aware, the use of mobile fingerprinting technology has always been sold on the basis that it does not create further significant infringements on personal privacy either through creating a separate database or retaining fingerprints. The technology has consistently been

¹⁶ *S and Marper v UK*, Application Nos 30562/04 and 30566/04, Grand Chamber judgment 4 December 2008

¹⁷ See paragraph 125.

presented as merely providing a speedier process for something that is already in existence. Increasing the number of databases holding intrusive biometric information increases security risks. With the government's recent history of data losses we urge strong caution in expanding the number of databases containing biometric information. It is also far from certain whether an additional fingerprint database could be justified in terms of necessity and proportionality, and it is clear that the creation of such a database would need parliamentary approval.

Links to other databases

13. The PIA states that the use of mobile fingerprinting technology could lead to wider access arrangements with other databases. It appears to be proposing extending access to other police databases (including the planned ID card scheme database) to those who carry the MIDAS device. Extensions in access to police databases cannot be analysed or approached purely in terms of convenience. The privacy implications of any database are dependent on who can have access to it: there is a huge difference between information retention and information dissemination. Any interference with an individual's right to private life must, under human rights law, be prescribed by law and be both necessary and proportionate. If it is envisaged that mobile fingerprinting technology will ultimately pave the way for greater information dissemination, a much more detailed consultation on these proposals is necessary.

Retention of additional biometrics

14. The PIA also suggests that the scope of MIDAS mobile devices might be extended to include images of palm prints and facial biometrics. This raises grave concerns not least because of the lack of detail provided. It is unclear from the PIA whether the creation of a whole new set of national biometric databases is proposed or whether it is intending to link the mobile technology to existing biometric databases held by other public bodies – for example the passport database. Either way, despite its casual phrasing, the PIA proposal would have far-reaching implications for the private sphere. The creation of new national biometric databases or indeed the wholesale extension of access to those that already exist would at the very least demand full parliamentary debate and approval. Any broadening of access justified on the basis of available technology that has not been legislated for by Parliament

and which is not properly regulated could easily lead to misuse and inappropriate use of powers.

15. As we have explained above, proposals such as these cannot be justified purely in terms of convenience and technological capabilities. As well as the privacy implications that attach to increased use of intrusive biometric data are important considerations about the relationship between the individual and the State. Expansion in the scope of biometric data checks to include palm prints and facial biometrics etc may also damage relations between the police and the public. This is recognised to a limited extent in the PIA at page 19: "*The public may have general unspecified concerns relating to intrusiveness and surveillance in society at large causing a reaction against this perceived further step towards an 'Orwellian' environment in the UK*". Our recent polling on this issue supports the view that the public are increasingly concerned about the level of surveillance in their daily lives. For instance, in a Liberty-You Gov opinion poll conducted in July 2009, 77% of respondents stated that they felt that the UK had become a surveillance society.¹⁸ Trust and confidence between the public and the police is a vital part of crime detection and prevention helping to ensure that crucial information and intelligence reaches law enforcement bodies. The slow creep of more intrusive methods of 'on the spot' identification may well undermine this important and sensitive relationship.

Extension of Lantern to children and young persons and those suffering from a mental illness or vulnerability

16. The consultation proposes extending the 'consent based' use of mobile fingerprint technology to children and young people and those suffering from a mental illness.¹⁹ While the consultation recognises inherent problems of using 'consent based' mobile identification with these groups it states that "*it does not seem reasonable that they should be deprived of the benefit that the capability may deliver*".²⁰ We are gravely concerned that, having already extended the practical application of their powers beyond what is provided for in statute through this supposed 'consent based' approach to mobile fingerprinting, the police, recognising the obstacles to using consent, appear to be seeking to extend their powers yet

¹⁸ See <http://www.liberty-human-rights.org.uk/news-and-events/1-press-releases/2009/30-07-09-another-home-secretary-another-id-card-launch-as-public-support-f.shtml>

¹⁹ See MIDAS & Lantern Equality Impact Assessment Consultation Paper, pg 8.

²⁰ Ibid.

further. Liberty believes that by adopting a purported 'consent based' approach to mobile fingerprinting, police are failing to restrict themselves to the intentions of Parliament. In respect of children, young people and those suffering from a mental illness who are unable to give true consent to having their fingerprints taken, this use of mobile fingerprint technology does not bear scrutiny.

Children and Young Persons

17. The consultation suggests that as persons who are 16 years or older may be served with a section 27 Notice under the *Violent Crime Reduction Act 2006*, the use of mobile identification for this age group '*would seem appropriate*'.²¹ We do not agree that there is an automatic link between a section 27 Notice and the appropriateness or otherwise of mobile fingerprint technology. Section 27 Notices are issued by officers in order to remove an individual (who is over the age of 16) from an area when the presence of the individual in that locality is likely, in all the circumstances, to cause or to contribute to the occurrence of alcohol-related crime or disorder, or to cause or to contribute to a repetition or continuance there of such crime or disorder.²² The fact that the police have coercive powers over young people does not in itself provide a premise for the blanket use of mobile fingerprinting for children with or without their consent. Currently, the police must gain the consent of both a young person (those aged between 14 and 17) and their parents in order to take their fingerprints.²³ For children under the age of 14, consent can only be given by a child's parent and not by the child themselves.²⁴ While mobile fingerprinting technology will be able to speed up the fingerprinting process once the relevant powers have been brought into force, it will not enable an officer to somehow gain consent from a young person's parents before taking their fingerprints.

18. As mentioned above, Liberty does not agree with the premise that a purported consent based use of mobile fingerprint technology is necessary and proportionate even when applied to adults who are capable of consenting. The problems with the use of the consent principle highlighted above are, however, even stronger when applied to children and young people. Children are vulnerable and

²¹ Ibid.

²² Note also current proposals in the Policing and Crime Bill to reduce the age for which a section 27 Notice can be served from 16 down to 10.

²³ See section 65(1) of PACE

²⁴ <http://www.yourrights.org.uk/yourrights/the-rights-of-suspects/the-rights-of-suspects-in-the-police-station/fingerprints-photographs-and-samples.html>

even more likely to feel intimidated by an officer asking for their fingerprints. Research has revealed that young people feel generally uninformed about police procedures, or the limits of police power and action.²⁵ Therefore a young person who, due to his or her age, is particularly vulnerable is unlikely to object to having his fingerprints taken when he or she is unsure of police powers and is concerned about the consequences of objecting.

Those suffering from a mental illness or vulnerability

19. The consultation suggests using mobile fingerprinting for those suffering from a mental illness or vulnerability.²⁶ The reason given is that this could prevent the police having to use section 136 of the *Mental Health Act 1983* (power to remove someone to a place of safety). The consultation states that its use would principally be in situations where no crimes have been committed.²⁷ Again, this approach demonstrates a sizable shift away from powers laid down in legislation, this time proposing the use of mobile fingerprinting technology where there is no suspicion of criminal activity. We understand the difficulty faced by police in dealing with vulnerable persons who may be distressed and in need of care. However, crime detection techniques and care and protection methods should not be confused. The principal purpose of the fingerprint database is crime detection and prevention. As such, PACE allows fingerprints to be retained and used but only for “*purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution*”²⁸. Use of the database must not be expanded to go beyond purposes laid down in legislation. We are particularly concerned that in proposing this extension to the scope and purpose of the database, the consultation displays seemingly little appreciation of the scale of the shift proposed.

20. As regards consent, the consultation explains that “*it is envisaged that officers would seek to obtain consent*” to use the mobile fingerprinting technology when dealing with those who appear to be suffering from a mental illness or vulnerability.²⁹ As with the use of this technology for children, the consultation displays a disturbing disregard for the principle of true consent. Those who are suffering from a mental

²⁵ See ‘Complaints from Children: the new police complaints procedure’, The Children’s Legal Centre, November 2006.

²⁶ See MIDAS & lantern Equality Impact Assessment Consultation Paper, pg 9.

²⁷ Ibid.

²⁸ See PACE, section 64(1AB) (b).

²⁹ See MIDAS & lantern Equality Impact Assessment Consultation Paper, pg 9.

illness and for whom an officer is considering using section 136 of the Mental Health Act – which allows for their removal to a place of safety where the officer believes that the person is in immediate need of care or control – will be unlikely to be able to give informed consent. It is also probable that an individual in this situation might be upset, confused or anxious. Although the consultation says that police will only obtain fingerprints where it will not cause a person to become anxious or upset,³⁰ it is hard to envisage circumstances where a person for whom section 136 might be invoked is not already in some sort of distressed state.

21. The consultation also lacks clarity as to when mobile fingerprinting should be used for those suffering from a mental illness. Although it suggests that using mobile fingerprinting may mean that an officer will be able to avoid invoking section 136, the consultation then explains that mobile identification will only be used in those cases where the terms of section 136 are not met from an initial assessment.³¹ It is therefore unclear in what circumstances mobile fingerprint technology will be used in respect of those apparently suffering from a mental illness or who are vulnerable.

Conclusion

22. As we have indicated, we have very real concerns with the way the MIDAS & Lantern project is currently operating and warn against rolling this out further. In particular we are concerned by the statement in the PIA that the MIDAS Project has entered into a procurement phase and that a contract will be entered into in October 2009 with a national service being delivered in Spring 2010. We believe there needs to be much greater debate about the use of this technology in the circumstances described before this goes any further. The relevant sections of PACE should be brought into force as a matter of urgency if forces wish to use mobile fingerprinting technology, and the purported 'consent' based approach to the taking of fingerprints should be discontinued. We also believe this is a matter for which the Government needs to take greater responsibility. It should initiate a review of the current system and conduct a full and proper consultative exercise to determine the proper boundaries of police conduct in this very sensitive area.

Rachel Yates

³⁰ Ibid.

³¹ Ibid.