Unite response to the Defra Consultation on the Proposed EU Emissions Trading System from 2013.

1 Introduction

1.1. **This response is submitted by Unite Amicus Section. Unite is the UK's largest trade union with 2 million members across the private and public sectors. The union's members work in a range of industries including manufacturing, financial services, print, media, construction, transport, local government, education, the health service and not for profit sectors**.

1.2. The Civil Air Transport (CAT) membership of Unite, is currently split between two Trade Groups. Together they are the largest trade union represent 80,000 employees employed in the United Kingdom (UK) aviation industry. These Trade Group represents workers in all areas of civil aviation except for flight deck and air traffic management.

1.3. Unite is currently debating the effects of the introduction between its trade groups as one group is resolutely against the introduction, whilst the other is still undecided. As a result this responses intends to set out the key points of the arguments raised by both contingents.

2 How will the Scheme work?

2.1. Unite believes the understanding of the scheme, in the public eye is portrayed as one which seeks to increase the security of the individual by combating the rise in identity theft and increasing security of sensitive and other areas by enabling law enforcement and security officials to obtain proof positive of someone's identity. This is achieved by recording biometric details of that person on a computer chip embedded into a card, which can be carried by the individual.

2.2. The key problem with this portrayal is that technology has reached the stage where these chips could store not just the information necessary to identify the individual, but additional information on that person's activity. These activities may well be political, social or financial and hence felt by many to be delving too deeply into that person's personal space. It is understandable that some agencies would want to ensure that criminal or anti governmental political details are held on such cards but nowhere so far has the line been clearly draw over the drawn as to what offences will be recorded, if any, and what would be considered to be anti governmental action. Would membership of a trade union be considered to be anti

governmental for example? Would details of the personal finances be included or purchasing habits?

2.3. Then there is the issue of security of this information. As we have seen all too often of late, there have been a considerable number of breaches in government security, enabling personal details to enter the public domain. Of major concern is the accessibility of the information to anyone who obtains these cards.

2.4. Recent figures on stop and search, especially amongst the Muslim Community, have dramatically increased. It is felt that members of the black community are more likely to be asked to produce ID Cards as proof of identity to the Police. The powers of the Secretary of State to compel registration in clause 6 of the Bill are likely to disproportionately affect black and minority ethnic communities, as they are likely to be targeted initially for compulsory registration for the purposes of enforcing immigration controls. The potential for clause 6 to be applied in an arbitrary and discriminatory fashion is not reduced by safeguards.

2.5. There will always be resistance by some in having their details recorded in this fashion. The public would clearly also wish to know the level of penalty faced if they refuse to subscribe to the scheme. If ID cards become the main proof of identity would be denial of basic services, may well encourage the development of an underclass that have little or no interaction with the state and are therefore, more open to exploitation. This has been the experience in France with regards to the so-called 'sans papers' – an underclass of people without an identity card who have no access to basic services.

2.6. Although Unite like many membership based organisations has a membership card with a unique registration number it does not require details of associations outside the workplace. Equally membership of a trade union can in some instances lead to the employer covertly treating the member differently. Although there is legislation to protect the individual from such discrimination, it requires proof sufficient enough to prove on the balance of probabilities that this is happening.

2.7. Membership organisations may therefore wish to ensure that access to details of membership would be clearly restricted to those organisations that have a definitive need to know, only.

2.8. Although the amount of data stored may well be limited by the Identity Cards Act 2006 it only takes an amendment to that bill to allow additional data above and beyond what is required to establish identity, to be stored. Due to the development of computer based technology especially data storage on smaller and smaller chips, the innate fear is now over the additional data would such an ID card chip has the potential of holding. Today's data storage devices enable the entire Encyclopaedia Britannica 2008 Ultimate Edition and several hours of video to be stored on to a memory card no bigger than nail on your little finger[1]. Critics of the scheme often site George Orwell's big brother state. There is no doubt that the technology is now with

[1] The Encyclopaedia Britannica 2008 Ultimate Edition uses 3.8 GB of memory, Micro SD card's are now widely available up to 16 GB with 32 GB and 64 GB versions being rumoured.

us to enable what could be beyond that needed for security purposes. Although some have the attitude that there is no need to worry if there is nothing to hide, there is the fear arising from the abuse of this technology.

2.9. For there to be wide spread acceptance these fears of the intrusion of privacy, the big brother state and the security of the data held, need to be overcome.

2.10. As with any technological revolution, there will be an innate fear as happened in the past with the mechanisation of the workplace, the introduction of computers, the internet and even decimalisation and the move to the metric system. Whilst some will willingly accept the transition others will resist until they have little or no option.

2.11. Unite believes that the general publics perception of ID Cards needs to undergo a significant amount of positive enforcement to overcome this resistance. The provision of help-lines and web page access would help, but first you need to convince the organisations, be they within government or otherwise, who may be involved with the implementation that the scheme is both secure and not open to abuse.

2.12. The Bill places an onerous burden on the individual to keep his or her information up to date (a civil offence punishable by a fine of up to £1,000), a provision which is likely to have a severely disproportionate and adverse effect on some of the most vulnerable groups. Examples of these include people with a mental illness or addictions; homeless people; older people; immigrants and asylum seekers; and those fleeing domestic violence.

2.13. The lack of a corresponding duty on authorities to ensure that entries are accurate results in a fear that errors by authorities would leave irreparable damage to ones reputation and possibly even their liberty.

2.14. Unite believe that the trade union movement would have a clear role to play in the provision of this advice as it often to the movement that members turn for advice. Before the unions do so however they need to be convinced that the benefits out weigh the disadvantages. Equally legal support organisations such as Citizens Advice, and the legal profession generally would have to be convinced, especially if they are to advise clients that there is nothing to fear.

2.15. At present if a person wishes to prove his identity the ultimate measure is to provide a passport or drivers licence. But how do you ensure that these are genuine?

2.16. Identity theft today is very easy to perpetrate. All a person needs is the full name and place of birth to obtain a copy of a birth certificate if the certificate was first issued more than 50 years ago. It is only where the individual is under 50 that there is a need for the date of birth to be provided together with the parents full names. With this the individual can send a completed form to the IPS and obtain a passport. Biometric data encoded into modern passports enables the document issued to be uniquely linked to the applicant for that document. There is no guarantee, however, that the applicant is the individual in whose name the application has been filled.

2.17. For their to be a way of ensuring a persons identity is not stolen all biometric information would need to be cross referenced with every other entry on the database to ensure that there is no duplication of biometric information with different applicants using different details.

2.18. Biometrics are not perfect either. No two fingerprints from the same person will be 100% identical, due to the amount of pressure used and surface upon which the print was left. As a result fingerprint matches are done on a probability basis were an operator identifies as many points of communality and features of a print as possible and compares their location and proximity to provide a score. Given enough entries therefore it is possible for two individuals to share a very similar print. Digitising fingerprint information reduces the quality of the original analogue print and makes false positives more likely. This occurred in the US when a FBI's erroneous fingerprint analysis of the fingerprint records of Brandon Mayfield linked him to the Madrid, Spain train bombings.

2.19. The chances of this happening again are remote and if additional biometric data is collected the chances of a reoccurrence of Mr Mayfield's case can be reduced.

2.20. A security researcher has demonstrated recently as a proof of concept that the use of a biometric keylogger[2] that can provide data to a potential hacker which they can analyze and re-use to subvert biometric systems and gain entry to secured buildings. Additionally a report from Information Risk Management[3] has shown that at present the number of false positives and negatives are quite high using some electronic biometric entry systems. As such the recording of all 60,943,912[4] individuals fingerprints

2.21. The government in this ID roll out is suggesting that the biometric information will be no more than a digital record of fingerprints and a portrait photograph. If additional data was used such as retinal or iris scans and a DNA fingerprinting, the chances of false positives fall into the realms of impossibility.

2.22. Iris scans analyze the features that exist in the coloured tissue surrounding the pupil which has more than 200 points that can be used for comparison, including rings, furrows and freckles. The advantage with retinal scans is that the detectors can distinguish between coloured contact lenses and the naked eye as an iris tends to be flat as opposed to the inevitable curve of a lens. The disadvantage therefore would be to contact lens wearers as they would need to remove their lens every time their eye was scanned. There is also no extensive evidence to suggest that irises staying the same with age, however, which could lead to problems over time.

2.23. Retinal scans use the arrangement and layout of veins at the back of the eye. If a person suffers from high bold pressure or some other medical conditions the shape of these vein patterns can change, however, adding more wrinkles in the path of these vessels.

---

[2] A device that scans a fingerprint into a computer to convert it into a digital password file.
[3] http://www.irmplc.com/index.php/75-What-are-BioMetrics---The-Executive-Summary
[4] Estimated information obtained from the FBI world Fact book - https://www.cia.gov/library/publications/the-world-factbook/geos/uk.html

2.24. Although DNA fingerprinting would provide a far more secure way of ensuring that person is who they claim to be, it requires several hours of laboratory processing to obtain a result.

2.25. Although the Data Protection Act 1998 does seek to provide a measure of security in creating a legal obligation of the collection and distribution of information about the person, as the scheme envisages the ability of the individual to readily be able to access and amend a proportion of their data, it opens the door to electronic hacking of the records.

2.26. Unite believes that the oversight of a scheme containing such sensitive information needs to be conducted by an organisation which is in the eyes of the public, secure and beyond reproach, answerable to government and the people for its actions. The failures of some government regulators to carry out their remits even when contained in legal statute have caused many to distrust these organisations motives.

2.27. As recent the recent BERR review has revealed, Postcomm has apparently ignored its primary obligation to preserve the Universal Service Obligation[5] focussing more on its secondary role of introducing competition, which has resulted in significant financial losses to the Royal Mail and the public purse whilst rival providers post significant profits. The Treasury Select Committee said that failures in the financial services regulatory body caused the run on Northern Rock, which ultimately lead to its collapse. Even in the aviation industry where this scheme is to be initially trailed, a committee representing airlines using Stansted Airport has said it had "lost confidence" in the Civil Aviation Authority's (CAA) ability to regulate. The Stansted Airline Consultative Committee (SACC) said the CAA was guilty of a "litany" of failures.

2.28. Involving the public in the scrutiny and oversight of such a scheme may well be very difficult to achieve. Examples of where public feedback has worked include the Law Society, Office of Fair Trading and Association (OFT) of British Travel Agents (ABTA). In the case of ABTA, its bonding scheme is the standard for the industry. Although the office of information commissioner already exists, knowledge of its existence is not as high profile.

3 Implementing the National Identity Scheme

3.1. To obtain an airside pass a worker already has to provide a passport and other form of id and have a police security check. This process takes time to obtain and this cost has to be bourn by the worker in question in most cases. The estimates provided on the cost of these ID cards have been estimated in the delivery plan to be around £30 per card. It has been suggested that the future application for airside passes will need both a passport and an ID card by the passing of an amendment to the Airports Act. This would create additional delay and additional red tape prior to a new employee being allowed to work airside, thus making the provision of such

[5] The Universal Service Obligation is the obligation currently held by the Royal Mail group which charges them with the obligation to provide a universally charged next day delivery service of mail to all citizens in the Great Britain regardless of their geographical accessibility.

ID cards compulsory. If the data collected for the ID Card is being conducted by the same department that issues passports, it begs the question, where is the added security and benefit to the security regime of such a move?

3.2. It is already the case that airside workers are subjected to a very high level of security not found on any other mode of transport. Workers are having their packed lunches tasted; to have their tool bags examined, not once but on numerous occasions as they go about their jobs. Airside measures which are now interfering with the operation of their duties creating significant delay and costs which the airport operator has to shoulder. A simple sweep of a runway for debris can cause the employees to endure six separate security checks, during which time the runway is non operational.

3.3. Despite the events on the 7/7 security measures have not improved significantly on London's underground network or on its busses. Indeed as current security measures stand it is possible for a barge with a shipping container of high explosives to go unchallenged up the Thames, from the sea and anchored outside the Houses of Parliament provided it makes no attempt to enter a port.

3.4. Additionally despite security measures being implemented at our airports, protesters were able to climb on the roof of an aircraft at Heathrow and climb onto the roof of the Houses of Parliament. As any security expert will tell you, there is no such thing as a 100% secure location, as the most determined individual will still find a fault in the system.

3.5. Lapses in security will always occur where human beings are involved, as we all have weaknesses, lapses in judgement and off days where due to fatigue or some other reason our mind is not on the ball. This does not mean that improving security would not reduce the risk of such lapses, but can rule out lapses altogether.

3.6. At present Counter Terrorist Security checks into workers who are from other European member states are far less rigorous than those on the domestic UK workforce due to delays and difficulties in obtaining information from the respective police forces. As a result there is no consistency in the airside badge process.

3.7. Fears are therefore rife that if a strict uncompromising security regime was introduced before an ID card was issued, that the ability to work airside may be delayed for months, while this information is obtained. Equally, however, there is the fear that workers who have obtained airside passes may be a security risk. To overcome these issues would require greater international involvement in obtaining this information.

3.8. There are clearly a number of technical and civil liberties hurdles that need to be overcome before the endorsement of a fingerprint identification enrolment capability.

4 Conclusion

4.1. Unite are happy to work with government to overcome the hurdles that are thrown up by the collection, storage and distribution of individuals data in this manner. At present however the union cannot see technical, practical or moral solutions to the problems that arise by its implementation.

Brian Boyd
National Officer
Unite the union
John Smith House
145-165 West Regent Street
Glasgow
G2 7RZ

Steve Turner
National Secretary
Unite the union
Transport House
128 Theobalds Road
Holborn
London WC1X 8TN

For further information please contact Colin Potter, Research Officer in the Unite the union Research Department on 0207 780 4011, colin.potter@unitetheunion.com