TØI report 914/2007
Authors: Torkel Bjørnskau, Mattias Gripsrud Tonje Grunnan
Tore Leite Dag Wiese Schartum
Oslo 2007, 108 pages Norwegian language

Summary:

Transport security and the protection of privacy

Security increase after 9/11 2001

The 9/11 terrorist attacks in the US have resulted in a number of new regulations and anti-terrorist measures in the transport sector. The added effects of subsequent attacks, against the railway in Madrid in 2004 and against bus and underground transport in London in 2005, together with revelations of terrorist bomb plans, such as those against transatlantic flights in 2006, have put security high on the agenda and resulted in a number of new anti-terrorist measures. Some of the most important of these are:

- intensified security checks of passengers and baggage at both international and national airports;
- introduction of biometric passports (mandatory for entry to the US);
- obligatory handover from airlines to American authorities of passenger lists with personal information;
- regulations and checks to prohibit the carrying on-board of more than 10 ml liquid (including bottled water) from outside the airport;
- testing of invasive whole-body scanners to check passengers (for instance at Chisholm airport, Amsterdam);
- introduction of fingerprint registration to check consistency between the those passengers boarding planes and those checking in baggage;
- intensified security demands for ships and ports including terrorist alarms, on-site checks, obligatory security plans and security equipment;
- stricter demands on securing ports and port areas by measures such as fences or admittance checks (the ISPS-code);
- stricter identity-card requirements for ship and port workers;
- security checks of employees in transport companies (control of personal history);
- security control of containers, scanning techniques, development of smart containers (RFID-marking), satellite based tracking systems and so on; and
- attempts at airport-style security checks on the London underground.

The report can be ordered from:
Institute of Transport Economics, Gaustadalleén 21, NO 0349 Oslo
Telephone: +47 22 57 38 00 Telefax: +47 22 60 92 00

Such measures imply that increased security efforts have been focused mainly within aviation and shipping, the two main transport modes in which security has been high on the agenda for a long time. It seems that the new terrorist threat has been given most attention in domains where there already existed high-profile security efforts, and that the threats have been countered to a lesser extent in those modes of transport in which security has traditionally had a less elevated profile.

Across all four main transport modes efforts exist whose primary aim is not to secure against terrorist attacks, but which nevertheless can be used to help unravel terrorist plans and prevent terrorist acts. One example of this is the use by British police of the system known as Automatic Plate Number Recognition (APNR) to track down one of the suspects of the car bombs at airport terminals in London and Glasgow in the summer of 2006. Other measures open to exploitation by the authorities for use in anti-terrorist activity include surveillance or registration of persons or vehicles, where the primary aim is to enforce speed limits and avoid petty crime; camera surveilance of terminals, vehicles, infrastructure and station areas (camera surveillance of public places is particularly widespread in Great Britain, but it has increased also in Norway over later years); automatic registration systems that register vehicle passes on toll spots (AutoPass); electronic tickets; intelligent speed adaptation (ISA); systems that automatically alert ambulance and police of road accidents (e-call); and automatic trip recorders in cars ("black boxes"). In Norway, there are plans to introduce automatic speed control over longer stretches of roads, using two or more speed cameras to estimate average speeds over the distances. In fact, within road traffic there are lots of new technological devices being developed and introduced to guide and control traffic, and it is not difficult to envisage their potential use in anti-terrorism efforts.

In light of this, these latter measures and systems can be considered alongside those more direct anti-terrorist measures as having obvious and important implications concerning the protection of privacy and data.

Anti-terrorism security in Norwegian transport – adaptation to international regulations

Security measures against terrorist acts in Norwegian transport are almost exclusively implemented as a consequence of international regulations. Aviation and shipping are the transport modes with the most comprehensive international regulations administered by ICAO, IMO and, increasingly, the EU, and it is within these transport modes that security efforts against terrorism have been intensified in Norway and most other western countries.

There are few independent Norwegian initiatives on anti-terrorist security measures in transport. The main aim of any security efforts that are implemented is to reduce ordinary crime, like vandalism and violence, and not to secure against terrorist acts.

Copyright © Institute of Transport Economics, 2007

Two main strategies for anti-terrorism security

There are two main strategies for security against terrorist acts. The first is that one can try to secure threatened objects and thus deter or prevent terrorist attacks. This is the main security principle in aviation, where all persons and all baggage must pass strict security checks in order to make sure that illegal and potentially harmful objects are not brought on-board planes. This strategy is very restrictive, however, meaning that even pilots must pass the security checks.

The second strategy involves securing against terrorist attacks by way of police methods such as surveillance of potential terrorist groups. The aim here is to take action against potential terrorists before they are able to attack. Such a strategy is more general in that it does not aim at securing specific objects, but rather at arresting the terrorists regardless of the object they plan to attack.

Conflict between security and the protection of privacy

The notion of the protection of privacy is associated with core democratic values such as civil rights and legal protection. It is concerned with the right to personal privacy and integrity, as stated in the Euorpean Convention on Civil Rights and in the EU’s Directive on the protection of personal data.

The term ”privacy protection” is normally associated with the protection of personal integrity, whereas the term ”data protection” connotes the protection of information of individuals. Originally, the focus was mainly on privacy protection, but with the introduction of computers and data storing facilities during the 1970s, data protection came increasingly into focus.

Security checks challenge personal integrity

The two security strategies mentioned above have different implications for privacy protection. Objects are secured by way of admittance control through physical scanning or inspection to prevent people from bringing in weapons or other illegal objects into a secure area. Such security checks threaten the protection of privacy mainly by challenging personal integrity. Physical checks or the use of scanning technology may be perceived as an invasion of privacy.

On the other hand, because security checks apply to all (it does not matter who the persons are), the strategy of securing objects by way of security checks is independent of person information and person registers. Thus, data protection rights are not challenged by security checks.

Surveillance and registration challenge data protection rights

It is clear that regstration and surveillance of people considered to be a security threat can violate their data protection rights. Such a security strategy must be based on the collection and processing of vast amounts of data that may lead to closer scrutiny of persons and groups by way of surveillance, stakeout and so on.

Copyright © Institute of Transport Economics, 2007

This strategy challenges mainly data protection rights in that a lot of personal information is collected, processed and stored. The right to personal integrity might also be considered violated for people subjected to closer scrutiny, but the majority of people, who are not examined closely, would probably not consider the surveillance and registration systems as a threat to their personal integrity.

To the extent that object control is accomplished by use of electronic equipment, or there are other types of information collection during security checks, data protection rights and personal integrity rights should be considered together. The use of for instance biometric methods and body scanners suggests that there will be closer links between these two aspects of personal privacy issues in the future.

Balancing security with the protection of privacy

The interest in privacy protection

Questions about privacy protection in the scientific literature often refer to the so-called ”Theory of interests”. This theory is an attempt to systematise and delineate the notion of privacy protection. The theory of interests consists of a number of specific interests that, when considered together, are assumed to represent our interest in the protection of our privacy. According to the theory of interests we have the following main categories of interests:

a) The interest in deciding about information concerning oneself.

b) The interest in inspection and knowledge.

c) The interest concerning the quality of information and information treatment.

d) The interest in balanced control.

e) The interest in user-friendly treatments.

f) The interest in person privacy analysis.

Point (a) implies that we have an interest in deciding what type of information about ourselves is going to be available to the authorities and others. In many respects this interest is looked after by the obligatory demand that people must consent to having their personal information collected and stored. Point (b) implies that individuals must have access to and knowledge about any of their personal information collected and stored. Point (c) states that as individuals it is also in our interest that the quality of the information collected and the treatment of this information is good. This also implies that it is possible to correct errors in the information collected. Point (d) maintains that there must be a balance between the type and amount of information collected and the purpose of the data collection. This point also implies that alternative and less thorough registration and control should always be considered.

Point (e) about user-friendly treatment implies that information about relevant registers, about procedures for data collection and data storage, about the governing rules and legislation should all be easily accessible and intelligible.

Copyright © Institute of Transport Economics, 2007

Point (f) ”Interest in privacy analysis” is added here as a specification of the interest theory with particular relevance to security measures in transport. This implies that considerations of privacy should be closely addressed when measures (such as security measures in the transport sector) are planned and adopted. It follows for instance that traditional impact assessment studies should be carried out when security measures are adopted, that the measures should be subject to consecutive control, and that cost/utility studies of the counter-measures should be carried out.

Security measures against terrorist attacks may threaten privacy rights

It seems rather obvious that in many cases points (a)-(f) are violated when anti-terrorism security measures are adopted. As noted, the surveillance strategy in particular requires secret registration, which is registration without consent and without any opportunity for the person being registered to gain knowledge about the information collected. Secret registration implies violation of not only data protection rights but also the interest in the quality of information and information treatment. When the persons themselves are not allowed to check the information collected, they cannot of course correct it for mistakes and errors.

The likelihood of achieving balanced control is also rather slim when one does not know what information is collected and stored. This is a particular problem when the aim is to secure against terrorist attacks where it is almost impossible to know beforehand what information might become relevant. Consequently, it is impossible to decide whether the informtion gathered is in balance with the aim of the registration.

User-friendly treatment is also hard to achieve where security measures are concerned. As noted, most security measures adopted in Norway are implementations of international regulations. The international regulations to prevent terrorist attacks against civil aviation were adopted through amendment to the Norwegian Aviation Act. This amendment addresses five different EU decrees and gives supplementary rules to these. Several of the decrees have been altered repeatedly and several have appendices that have been classified as closed to the public.

Secrecy and limits to insight violate fundamentally the principles that otherwise dominate the areas of data and privacy protection. What replaces them is merely the hope or expectation that authorities and control actors will behave according to human rights principles and according to national law. However, to trust actors to behave according to the law without being able to check their actions because of secrecy is a severe problem within a democratic constitutional state.

The comments on the theory of interests presented above clearly show that the security measures adopted within the transport sector, and within other areas, almost without exception violate the principles of personal privacy and data protection. It is, however, to some extent possible to compensate for this by strengthening legal protection.

Much of the law concerning privacy and data protection rights already comes in the form of procedural rules and principles that describe the proper way to collect personal data. Modification of these regulations to effect a very specific description of what personal information can be collected, used and registered in order to conduct security checks for instance in the transport sector would make the control process more predictable and easier to check, and thus make the control regime more acceptable according to privacy and data protection rights.

An added advantage of such a procedural approach is that it implies the utilisation of technology to the greatest extent possible to make the control objects anonymous or pseudonymous. Security checks should accordingly to the greatest extent possible be carried out without revealing a person's (real) identity. From the perspective of personal privacy one may argue that personal data should be collected electronically and/or automatically rather than manually. The reason is that privacy rights are better fulfilled when the information is not available to other persons.

Naturally, security measures against terrorist attacks must at least partly be based on secret surveillance and registration. In compensation one may adopt stricter rules concerning the procedures, the treatments and the storage of person information. For instance, one can possibly ban the use of certificates of conduct older than five years, adopt minimum standards of identification and authentication when a case is brought to trial, guarantee independent expert scrutiny of information systems that have provided unfavourable information, and identify legal responsibilities for unlawful collection of person information.

Views of Norwegian transport actors on security and the protection of privacy

Representatives from the four major transport modes, together with representatives from relevant authorities, were interviewed about security measures adopted in the transport sector. They were asked about possible implications for personal privacy and data protection, how they weigh security and privacy issues against each other and how security issues are founded in their organisation.

Representatives from the following organisations/bodies were interviewed: Oslo T-banedrift (The Oslo Underground), Oslo Havn (Oslo Port), E18 Bjørvika, (Project organisation within the National Road Administration being responsible for the construction of the subsea Bjørvika-tunnel in Oslo), Datatilsynet (The Data Inspectorate) Nasjonal sikkerhetsmyndighet (The Norwegian National Security Authority), Kystverket (The Norwegian Coastal Administration), Jernbaneverket (The Norwegian National Rail Administration), NSB (The Norwegian State Railways), Luftfartstilsynet (The Civil Aviation Authority) and Vegdirektoratet (The Directorate of Public Roads/National Roads Administration).

Differences between transport modes determine security efforts

The respondents were of the opinion that differences between the transport modes were of great importance for the level of security attention. One aspect mentioned was that urban mass transport has so many passengers, departures and stops/stations that it is practically impossible to adopt an aviation-style security

Copyright © Institute of Transport Economics, 2007

regime. Such a regime would also be far too costly for most urban transport companies.

Profound differences were observed between the transport networks that the different transport modes operate in. Aviation is characterised by centralised point-to-point traffic, where airports are placed outside of central junctions and thus much more easy to secure physically than, for instance, railways and underground systems. Road traffic is characterised by very open access and it is almost impossible to imagine security checks and control of access to the road system.

A related aspect concerns the level of integration of the transport system with society and everyday life. Tram lines with frequent departures in Oslo are called ”rolling pavements” which illustrate how trams (and buses/underground) are perceived as an integrated part of city life. Massive security checks of passengers is something that is perceived as incompatible with a vital city life.

Several respondents also pointed out that there are huge differences in risk acceptance between transport modes. Aviation deviates from the other modes in its very low level of risk acceptance and consequent high security costs. Several respondents argued that safety for society as a whole would increase if resources were transferred from security measures in aviation to ordinary safety measures in road traffic.

Several respondents also maintained that the institutional basis and governing rules of different transport modes influenced to a very large degree the scope for instigating and adopting security measures. For instance, aviation and sea transport are heavily regulated by international agreements and the different transport companies and infrastructure administrations have no choice but to comply with these international rules.

Privacy implications for employees and transport users

The respondents have different perceptions both regarding *whether* the measures implemented have privacy implications, and for *whom* they have implications. Within road transport privacy questions are perceived as more relevant to employees than to road users. Within aviation, however, privacy issues in association with security measures are perceived as something mainly affecting the passengers.

The impression of The Data Inspectorate is that actors within aviation are very much concerned about questions regarding personal privacy when implementing safety and security measures. Similar concerns do not seem to be present within the other transport modes. It is of course mainly the security checks at airports that have privacy implications.

The Oslo Underground maintain that they are traditionally cautious when it comes to measures with implications for personal privacy, and that they abide by the rules. For Oslo Port, however, the main focus is to implement international regulations concerning port and ship security and questions regarding personal privacy are not much discussed.

Copyright © Institute of Transport Economics, 2007

The Norwegian Road Administration is mainly concerned with privacy issues regarding road safety measures where some kind of traffic surveillance is involved. This is particularly relevant to current ‘hot’ issue of speed enforcement by use of speed cameras calculating average speeds for single drivers over a specific stretch of road. The sub-sea tunnel project in Oslo has introduced access control to the site, and other security measures, but privacy issues have not been addressed to any large extent.

The Norwegian National Rail Administration (Jernbaneverket) manages infrastructure and is in that respect not much involved in privacy related issues. They nevertheless feel that such questions are relevant when it comes to security clearance of employees.

In the Norwegian State Railways (NSB) one is aware of the privacy implications of camera surveillance and has deliberately chosen equipment and procedures in order to avoid violations of privacy protection and data protection rights. Nevertheless, privacy issues are for the most part seen as relevant to their own employees.

The general impression is that privacy issues are not high on the agenda in Norwegian transport companies, but that actors have considered privacy implications of measures within their own organisation. No respondent felt that balancing privacy rights and security needs was a particularly big problem. The Data Inspectorate has intervened to prevent the use of some measures, but these measures have mainly been directed towards threats other than possible terrorist acts.

Perceptions of security and safety today and in the future

Norwegian transport companies are familiar with the distinction between safety and security. Some include measures against ordinary crime, such as vandalism, tagging (graffiti) and theft, in the security concept. Many feel that there is a close connection between safety and security, that security measures can have positive effects on safety. As regards emergency and evacuation plans, the distinction between safety and security is irrelevant: if fire starts one needs to have staff and equipment to put it out regardless of its cause.

The most important security measures with privacy implications that have been implemented are: camera surveillance of transport means and infrastructure, information measures, training, access control of passengers and employees, and inspection and physical protection of transport means and infrastructure. Everyone also mentioned close contact with the secret police service (PST). Advanced security measures like automatic face recognition systems, advanced x-ray equipment etc. were perceived as not very relevant, apart from in aviation, where respondents argued that security measures based on biometrics are of high interest.

Administratively, security is organized within traditional safety units both in Oslo Underground (T-banen), in the Norwegian National Rail Administration (Jernbaneverket), in the Norwegian State Railways (NSB) and in the Directorate of National Roads (Vegdirektoratet). Within the Norwegian Coastal Administration (Kystverket) and the Port Authorities (Havnevesenet), security

Copyright © Institute of Transport Economics, 2007

and safety are also placed together within the same units. However, in the Civil Aviation Authority, these issues are separated with a special unit responsible for security issues.

Within all transport modes, safety is systematically and continuously dealt with, for instance by use of risk and vulnerability studies. Possible terrorist attacks are a part of the threat scenario. Counter-measures against terrorist attacks have had the favourable side-effect of reducing ordinary crime.

Most actors identify the need for better coordination of security measures across transport modes, but they do not see the need for common intermodal regulations in this field. Most actors expect surveillance to increase in the years to come, but they do not envisage ”airport-like” security systems implemented in other transport areas, with the exception of sea transport and port security.

Security, effectiveness and legal rights

Terrorist threats and privacy protection issues are not high on the agenda in Norwegian transport. Most anti-terrorism security measures are implemented as part of adherence to international regulations, and transport modes that traditionally have been characterized by a lot of international regulations – aviation and sea transport – are also the ones where security measures have been most intensified and expanded recently.

Responsibility for security measures is to a large extent placed administratively in the same units that deal with ordinary safety issues. Further, these units carry out to a very large degree the sort of incident-based (i.e. after-the-event) counter-measures that are typical of ordinary safety work. These sorts of measures dominate security planning against terrorist attacks. Consequently, one ignores the fact that terrorists may select the targets where security is poorest. Incident-based security policies will normally have limited relevance when faced with possible terrorist attacks. Furthermore, it follows that strengthening security to already protected objects will have only a limited effect.

From a societal view it seems rather obvious that the heavy security regimes in aviation are out of proportion to the almost total lack of security efforts in other transport modes. It is a paradox that you cannot bring ordinary water bottles on planes and at the same time there is no security check, either of passengers or baggage, on the train or underground.

To secure specific objects against terrorist attacks is at best only “locally” rational. It may in other words merely transfer the risk to other objects less well secured. To society at large a strategy based on object protection will be both costly and of limited effect. In some transport modes, especially road traffic and public transport in urban areas, it will not be possible to protect the public effectively with such a strategy. Furthermore experiences from abroad indicate that effective counter-terror policies must be based on police methods like surveillance if terrorist attacks are to be prevented.

Security checks to protect specific areas or objects, such as security checks at airports, have obvious privacy implications. Body scanners, and body searches may be experienced as a violation to personal integrity. However, security

Copyright © Institute of Transport Economics, 2007

policies based on surveillance and registration of potential terrorists may have even more severe implications to privacy and data protection. Surveillance and registration will not only include data collection of a huge number of persons but implies data storage in data bases with the potential to link data from different sources, to leak information to unauthorized persons, to make incorrect registrations etc.

Securing specific areas or objects by access control and security checks is only a realistic option within aviation and sea transport. To secure other transport areas a comprehensive surveillance strategy may be envisaged. Such a choice, will however, have severe implications to privacy and data protection.

Giving controllers wide authorisation to collect and check information about us raises questions about how to control the controllers. One can easily imagine that controllers may see a certain level of terrorist threat to be in their own interest, in that more resources may be allocated to security as a consequence. While we have not experienced such problems to date, the situation is clearly far from ideal. It is easy to suspect that the security services overstate the terrorist threats.

These are not only challenges to privacy and data protection but rather to our democratic legal tradition. Secret police with wide authority and a monopoly on the information about terrorist threats, is something we do not associate with democratic legal states. Thus we must ask whether the actual threats we face can justify severe violations of privacy, data protection and legal rights.

Copyright © Institute of Transport Economics, 2007