International Working Group
on Data Protection
in Telecommunications

675.38.12 13 March 2009

Report and Guidance on Road Pricing

- "Sofia Memorandum" -

45th meeting, 12-13 March 2009, Sofia (Bulgaria)

Recommendations

The Working Group recommends that the designers of large scale road pricing systems which process personal data should comply with the following recommendations designed to protect the privacy of drivers and owners of vehicles:

- The anonymity of the driver can and should be preserved by using the so-called smart client or anonymous proxy approaches that keep personal data of the drivers under their sole control and do not require off-board location record-keeping.

- Road pricing systems can and should be designed so that the detailed trip data are fully and permanently deleted from the system after the charges have been settled in order to prevent the creation of movement profiles or the potential for function-creep.

- Processing of personal data for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible with clear and unambiguous consent from the individual.

- In terms of enforcement, the system should not ascertain the identity of the driver or owner of a vehicle unless there is evidence that the driver has committed something which is defined as a violation of the road pricing system.

Background

Large-scale electronic road pricing on a »pay as you go« principle in free-flow traffic is not a new idea. Thoughts on electronic road pricing emerged in the last decades of the 20th century[1]. Different terms are used to describe the use of modern information and communication technologies in road pricing and transport, such as "electronic road tolling", "intelligent transportation systems" (ITS), "electronic toll collection", "road-user charging", "time, distance, place charging", "distance-based road user charging", "vehicle miles travelled (VMT) charging" and several others.

Existing road pricing technologies can levy a toll on highways, can charge vehicles for entering a zone, but cannot compute so-called "time, distance, place charging" algorithms required for

Secretariat
Berliner Beauftragter für
Datenschutz und Informationsfreiheit
An der Urania 4- 10
D-10787 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

large-scale implementations. The desired outcome of an electronic road pricing scheme is the ability to charge for *actual* use (i.e. the more you drive the more you pay) depending on the time of journey (e.g. less during off-peak periods) and with a varying tariff according to the chosen road. Traffic flow may be enhanced because drivers are not required to stop at toll booths in such schemes. In principle, this is the fairest and ecologically the most desirable way to pay, just like consumers usually pay for water or electricity consumption.

Besides road pricing, there are several other services based on time, place and distance data, such as parking schemes, pay-as-you-drive insurance, parking finder/auction, road space rationing, parking loyalty programs, congestion mapping and congestion charging, travel advisory ("you could save 12 EUR per week if you left 30 minutes earlier each day") and intelligent transport systems (“if you use A2 motorway instead of A3 today, you will pay 20% less”). While electronic collection and processing of location data, identification data and charging data about individual’s journeys may and is already used for several purposes and raises several socio-economic questions, this paper focuses primarily on privacy implications of (large-scale) electronic road pricing.

To have a better understanding of what the privacy implications of electronic road pricing schemes are we need to take a closer look at some of the basic principles of the system. Large-scale road pricing initiatives that involve processing of personal data (i.e. other than vignette, anonymous tag and beacon and non free-flow toll-booth based systems) are being developed all over the world, for example in the US (Oregon and Puget Sound region), Australia, New Zealand, Canada (the 407 Express Route), the Toll Collect system in Germany[2] and road pricing plans in the Netherlands[3] and Norway. Furthermore, in the EU, the aim of the Directive 2004/52/EC is to embed the »pay as you go« principle in free-flow traffic in the future European Electronic Toll Service (EETS). In its final stage of development this trans-European system should provide toll charging for all types of roads, including viaducts, tunnels and other objects. With the new road charging system, drivers could pay the toll without having to stop and cause traffic congestion. Also, the same device should be able to levy the toll on all European motorways defined as payable.

The reason road pricing is so emotive is that it brings together location data, identification data and charging data: in other words, knowing who was where at what time, and charging them for it. In order to enable the »pay as you go« principle in free-flow traffic (and also to have one interoperable system) it is clear that road pricing schemes could entail massive surveillance of the movements of individuals (vehicle owners and drivers), therefore the implications for privacy of those individuals need to be carefully studied. It is not difficult to imagine the huge value of a centralized database of driver’s movement data and various function-creep scenarios where data might be exploited for purposes other than those for which the data were ostensibly collected (i.e. road pricing). Several information commissioners and data protection authorities have already issued opinions and guidance on privacy protection in electronic road pricing schemes (e.g. Ontario[4], the Netherlands, Victoria/Australia[5], New Zealand[6], Norway[7] and Slovenia[8]). Misperceptions of privacy implications are actually often considered as one of the most important deterrents for the implementation of large scale road pricing systems.

As far as technology is concerned, two mainstream technologies are envisaged for these systems: short range communications (DSRC[9]; also described as tag-beacon system) and global navigation satellite system (GNSS/CN[10]), which can determine the position of the car and transmit the data via high-performance wireless communication networks – the latter is frequently referred to as satellite road pricing system.

Each has its advantages and disadvantages: the DSRC-based solutions technologies, for example, are more widely used and have been more frequently tested but they are not suitable for all roads[11]. The choice of technology depends significantly on the implementation size and differs between relatively small-scale (e.g. metropolitan[12]) and large scale (nationwide or even international wide) implementation. Speaking from the viewpoint of large-scale implementations the DRSC-based solutions seem to be losing ground. Due to the enormous number of road segments to cover, solutions requiring substantial roadside infrastructure to determine the amount of road usage – as in existing DSRC-based systems – are less suited in cases where all roads are likely to be charged[13], a view which is also echoed in the recent report from the US National Surface Transportation Infrastructure Financing Commission[14]. The advantage of a satellite-based system is its flexibility, while on the other hand such systems have not been tested widely in practice.

The exploitation of electronic road pricing schemes is - leaving aside the vast socio-economic debates and consequences - often hampered by two common privacy misperceptions held by the general public and media that need to be firmly discarded.

Firstly, the Working Group emphasizes that there should be no concern that GPS-based approaches would mean building of an all encompassing database on the position of vehicles in a "big brother in the sky" style. The US GPS, Russian GLONASS as well as the future Galileo satellite positioning systems are based on passive receivers, which only calculate the location of the vehicle using satellite data, and these receivers cannot communicate the information on the location of the car back to the satellites. Therefore, in opting for a system of satellite-based road charging we need to understand that by satellite navigation a vehicle only obtains the information on its position, whilst the location data is transmitted to the control toll charging centre via wireless networks, such as for example the GSM network. An all encompassing database of location and identification data could therefore only exist "on the ground" in the control centres, which is exactly what this paper is dealing with.

Secondly, comparisons are frequently made with mobile telephony or credit cards, where individual's data is or may be tracked. The Working Group would like to point out that such simple comparisons are not appropriate, foremost because road pricing devices must remain in constant operation (at least on payable roads), unlike in the case of mobile phones the use of which is entirely voluntary. The ability to switch off the device on a payable road would facilitate payment evasion, and for this reason the privacy implications of road pricing schemes become even more relevant.

The distribution of the charging process

The charging process is split into four phases:

1. determining the position of the vehicle,
2. determining the segment of the road or toll element and the corresponding tariff,
3. calculating the amount due for that segment,
4. calculating the total amount due for the journey.

A crucial factor when estimating privacy implications is how the phases of the charging process are distributed between different data processors. The four phases of the charging process can

either be performed by one processor or they can be split between two or more of them. Consequently the privacy implications differ from one implementation model to another. Some of the models are presented below together with the most important elements that need to be considered when assessing privacy implications. The two principal models for road pricing are the **thin client approach** and the co-called **smart client** approach; however other models exist in between those two, such as the distributed role approach and proxies. These four approaches are discussed below

The thin client approach

The least favoured solution for electronic road pricing system, in terms of privacy protection, is where all data on journey time and position of vehicles are sent to or collected by a single body or institution acting as a control centre. The so-called thin client (or On-Board Unit – OBU) only collects the data on journeys travelled and all four phases of the charging process are processed by the control centre using a centralized database of location data, identification data and charging data.

The Working Group expresses its concerns about adopting this approach, since it clearly offers the least protection for the privacy of the individuals. In principle, the question of preferring thin or smart clients is a question of centralized vs. distributed processing, a dilemma often encountered in privacy and data protection.

The proponents of centralized processing claim that if data were kept centrally and protected by suitable data security mechanisms (e.g. appropriate access control, logging of personal data processing etc.), it would be possible to ensure a higher level of security than a single individual could ensure. A counterargument however is that where the data are under the control of an individual, only his/her own personal data remain vulnerable (e.g. if the vehicle or the road pricing on-board device was stolen), whereas in the centralised processing system personal data of all individuals are potentially vulnerable (despite a possibly higher level of security). For this reason, and from the viewpoint of privacy protection, it is necessary to favour those solutions where personal data are not kept centrally, but remain in the possession and under control of an individual. Furthermore, privacy advocates are frequently dealing with the so-called function creep phenomenon, where data originally collected for one purpose (which can be perfectly legitimate and lawful) is later used for another purpose, where access to data is possible by previously unforeseen third parties and so on. Function-creep worries practically vanish when data are processed under the control of the user.

The distributed-role approach

Some models propose the so-called distributed-role approach, which supposedly provides for better protection of privacy and personal data. The distributed-role approach is a solution based on the principle of sharing the data between two centres or parties, one of them having location and charging data whereas the other only has identification data of drivers.

The first centre or party has the identification number of the device in the vehicle and receives information on the route the vehicle has made (journey time and position), but does not know who the owner of the device is. Based on this information the centre calculates the fees due. Such aggregated calculations of data (only the sum of the toll within a certain time period, without information on journey time and position), are then sent together with the identification num-

ber of the device to another centre which can identify the owner of the device who is then charged with the toll, however, this second centre does not keep the information on the journey of the vehicle. The proponents of this approach often claim that this distribution of roles does not entail that personal data are processed; however the Working Group would challenge such reasoning, because a vast amount of personal data is still being processed by the centres.

This solution only apparently protects the privacy of an individual, even though one centre keeps the information on the vehicle positions and journey time and does not know the identity of the driver, and vice versa. Throughout this approach enormous amounts of personal data are still collected and processed centrally by one centre and only the identification data is trusted with another centre or party. The Working Group would like to echo the opinion of the Article 29 Working Party that data, relating to an identified or identifiable natural person, need to be treated as personal data and that the identifiability of an individual is not assessed only through the means and resources of a data controller (in this case the first centre) but should rather be assessed more generally. The controller should anticipate that the "means likely reasonably to be used" to identify the persons will be available e.g. through the courts appealed to (otherwise the collection of the information makes no sense), and therefore this information should be considered as personal data. Regardless of whether the first centre can or cannot identify an individual to whom the data on time and position refer to by itself, this centre undoubtedly processes personal data. To support this, it is evident that in case the road charges have not been paid, or the person has refused payment, the creditor will need to find a quick and simple way to reproduce the calculation of the toll which means that the data on journey time and position of an identifiable person will need to be processed. Furthermore, the function creep effect is again quite possible since large amounts of data are centrally stored.

The smart client approach

In order to ensure the privacy of individuals, clearly the most appropriate system would be the one in which the data needed for the purpose of road pricing, would be exclusively under the control of the user. In this case the calculation of the toll would be made by the device (the so called intelligent device), while the control centre would receive only the sum of the toll incurred. This means that all four phases of the charging process in electronic road pricing system would be processed by the device itself: determining the position of the vehicle, determining the segment of the road and the corresponding tariff, calculating the amount due for that segment, and calculating the total sum.

The anonymity of the driver would thus be preserved since all the data on the position and journey time would be kept under the sole control of the user. The users should only identify themselves if certain irregularities emerged in which identification would be required: for example, when the user has not paid a correctly calculated toll fee, or when the vehicle has been stolen, when the user's toll system device is broken down or malfunctioning (whilst driving on a chargeable road segment). The control centre only needs to be sure that the device in the vehicle which calculates the toll is working correctly on the roads on which tolls are charged.

In such a system the control centre does not have data on the position of the vehicle; it only checks whether the device is operating correctly. This system, of course, also requires some operational measures such as protection of the equipment from fraud (including jamming, tampering, shielding, tweaking, intentional malfunctioning etc.) One very important aspect of both thin and smart clients is that they cannot be switched off by the user when the car is on a payable road, since this would enable payment evasion. The smart client approach does not come

without challenges - it is for example necessary to provide suitable certification standards, proper installation and maintenance of such devices, and also consider some other technical aspects (e.g. power supply, checking correct functioning, memory capabilities), and probably the most important aspect – the costs.

While the smart client approach appears to be a more costly solution than the so-called thin client, the smart client approach also has certain economic advantages: the »intelligent« device is not sensitive to communication hindrances (e.g. areas which are not covered by GSM signal), or if the control centre is temporarily not operating since the system can process the toll itself. On the other hand, the device which continuously sends data (the thin client) to the control centre and relies on control centre's calculations cannot process the calculations of the toll by itself in the areas with poor GSM coverage, or when the central control is not working. It is also very important to mention that the intelligent device also supports operation in the thin client mode (metaphorically speaking the "dumb" client cannot become "smart" whereas vice-versa is possible), which is an especially important requirement when interoperability is needed (e.g. within the future European Electronic Toll Service) or with other pre-existing metropolitan toll collection or congestion charging systems. The devices in vehicles will need to know how to respond to different regimes: after entering the territory of another operator, the device will receive instructions on how to work. International standardisation organisations (ISO and CEN) are developing suitable technical standards, whilst the industry already has proven working solutions. While economic factors are clearly crucial for take-up of a certain system, they do not affect the privacy implications. The perceived cost penalty for a smart client could be minimised by mass production economies or incentives (e.g. by bundling an onboard hands-free mobile phone or satellite navigation system into the device).

A smart client could also facilitate anonymous use if pre-pay options, as currently provided for mobile phones, were offered. A driver should have the opportunity to buy toll credits which could be applied to the onboard unit, which could then advise the control centre that the charges for the payable road segment in question had been pre-paid.

Proxies

Other mixed-type approaches have also been known and are already available on the market. The charging centre can, for example, operate merely as a technical centre – a kind of an intermediate or proxy which has been selected to perform calculations. These proxies (usually dubbed as anonymous forwarding proxies or anonymous loop-back proxies) can be on or off-board and can have the functionality to store data on-board or not. Assessing the privacy implications of these approaches is in principle a matter of trust (i.e. whether the device can be trusted and whether the control centre or third parties are really unable to access personal data).

The Working Group is generally in favour of such proxy approaches provided that their privacy protection can be independently assessed and they meet the privacy protection level of a purely smart-client approach.

Enforcement

Enforcement is another crucial element that needs to be designed in a privacy friendly manner if we are to preserve the anonymity of the drivers in electronic pay-as-you-go road pricing schemes.

The area where possible abuse of personal data may happen, and requires special attention, is the implementation of surveillance and detection of offenders. The identity of the drivers must not be ascertained unless there is evidence that the driver has committed something which is defined as a violation of the road pricing terms of use or some other offence. The principle of proportionality should be fully respected, i.e. first of all it needs to be established whether the toll system device is present in the vehicle and whether it functions faultlessly. If the control unit does not detect any violations regarding the presence or proper functioning of the toll charging device, it should make no further steps for the identification of the device and the driver. Only if the supervising unit detects absence of the device, improper functioning of the device, or that some improper adjustments on the device may have been made, should the authorised body, according to the principle of proportionality, proceed with identification of the driver. According to reports of expert groups, number plate recognition process and thus identification of the individual driver or owner is an satisfactory method of control in this respect.

Considering all the above, the personal data of drivers who have not committed any offence should not be processed in any way except by the driver. Using this approach, the control centre would only check if the device in the car is functioning correctly, and only an authorised person (for the purpose for which this person has been given authorisation to access personal data) may request identification of the individual, or obtain information on the position of the vehicle. This may be permitted only in certain circumstances which need to be predefined and enumerated (for example if the electronic road pricing device in a car has been tampered with, or if the device was not working while using payable roads, or if the car was stolen). Every access to the information on the position, journey time and tolls for enforcement purposes needs to be suitably recorded, allowing an authentic and complete auditing tracing. It would be impermissible to allow unauthorised and unregistered access to the data in the device.

The question of optional or compulsory use

If the usage of an on-board unit is optional, the drivers can either use an on-board unit or choose a different method of toll charging and payment (e.g. by subscribing and paying the toll on an automatic station). What needs to be stressed is that in either optional or compulsory scheme the user cannot switch off the device while driving on a payable road. The question of optional or compulsory use of the road pricing device and the impact on privacy is to a great extent closely related with the question of surveillance. In principle, optional use is more user-friendly since individuals can give prior consent to processing of their personal data; however the enforcement issues are closely connected and should be evaluated as well.

An example from German experience for heavy vehicles (the TollCollect system) shows that 90% of truck drivers have opted for the installation of a satellite toll system and less than 10% prefer other systems. Reliability and accuracy of the installed systems is 99.75%, which means that virtually all problems of enforcement and irregularities occur with those without installed devices who subscribe and pay manually at toll stations. If we transfer this experience from heavy vehicles to a road pricing system for private cars (especially if it is to be eventually used on all toll roads), optional use seems less realistic. An optional road pricing system in free flow

traffic would require installation of very complex and expensive control systems on all payable roads (video surveillance, identification of number plates, etc.), which would consequently mean a high degree of surveillance and even greater encroachment into the privacy than in a compulsory system. The decision on whether to allow optional use or enforce compulsory use largely depends on the implementation size and enforcement resources and might differ in a small-scale and a large scale (nationwide or even international wide) approach[15].

Data subjects rights

Special attention should be paid to the questions of disputed charges. If we want to ensure that personal data remain fully under the user's control, access to the data should only be provided for if the user explicitly requests so. Road pricing systems can and should be designed in a way that the detailed trip data are fully and permanently deleted from the system after the charges have been settled and any period for disputing the charges has expired. (e.g. as happens in the London congestion charge system)

Remote access to raw data by the control centre or by third persons for purposes other than enforcement, regardless of whether the data are stored in the device or not, should only be allowed upon consent of the individual. Similarly, processing for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible if the vehicle owner has given his clear and unambiguous consent.

Conclusions

The Working Group is of the opinion that centralized processing of personal data for the purposes of road pricing in free-flow traffic is not necessary and is therefore unjustified under the principle of proportionality, given that proven technological solutions exist that do not require centralized processing of personal data. Strong privacy protection can and should be designed from the start so that the information transmitted to the control centre would only relate to the bulk charges due and would not include detailed data on time and place of travel. As pointed out in the report by the US National Surface Transportation Infrastructure Financing Commission, such a system would provide considerably more privacy than other information technology systems in our society, such as credit card and mobile phone systems, where the provider knows not just how much a person owes but where the individual made purchases and what phone numbers were called (more or less precisely even the location). Road pricing systems can and should be designed so that the detailed trip data are fully and permanently deleted from the system after the charges have been settled in order to prevent the creation of movement profiles and the function-creep effect.

The anonymity of the driver should be preserved throughout the functioning of the system. In terms of enforcement the system should not ascertain the identity of the drivers unless the driver has committed something which is defined as a violation of the road pricing system. Processing of personal data for other purposes (e.g. pay-as you drive insurance or behavioural-based marketing), should only be possible with clear and unambiguous consent from the individual.

In principle, the question of privacy in electronic road pricing systems is quite simple: any large scale road pricing system in its essence and purpose does require personal data processing but

does not require centralised personal data processing (so long as no offence has been committed), nor does it require disproportionate processing of personal data, access to personal data and ubiquitous surveillance. The fundamental principles of personal data protection strive for maintaining the anonymity of the driver and technology should and can be used in a way that preserves the anonymity of the driver. Any digression from this principle would represent an additional encroachment into already eroded privacy in the information society.

---

[1] Electronic Road Charging: http://www.parliament.uk/post/pn112.pdf

[2] It has to be noted that the TollCollect system in Germany is only used for trucks: http://www.toll-collect.de

[3] Ministry of Transport, Public Works and Water Management: Implementation of road pricing system. http://www.verkeerenwaterstaat.nl/english/topics/mobility_and_accessibility/roadpricing/index.aspx

[4] 407 Express Toll Route: How You Can Travel the 407 Anonymously. Information and Privacy Commissioner Ontario: http://www.ipc.on.ca/images/Resources/407-e.pdf

[5] An in-depth study of road pricing and an exhaustive list of sources were prepared by Victoria Transport Policy Institute: Road Pricing. Congestion Pricing, Value Pricing, Toll Roads and HOT Lanes. http://www.vtpi.org/tdm/tdm35.htm

[6] Road Reform and Privacy: Which Way Forward? Submission by the Privacy Commissioner to the Ministry of Transport in relation to the final report of the Roading Advisory Group: http://www.privacy.org.nz/road-reform-and-privacy-which-way-forward/?highlight=impact

[7] http://www.curacaoproject.eu/documents/newsletter-issue3.pdf

[8] http://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=568

[9] DSRC - Dedicated Short Range Communications.

[10] GNSS/CN - Global Navigation Satellite System/Cellular Networks

[11] Privacy-Sensitive Congestion Charging. Alastair R. Beresford, Jonathan J. Davies, and Robert K. Harle: http://www.cl.cam.ac.uk/~arb33/papers/BeresfordDaviesHarle-PrivacyAwareCongestion-SPW2006.pdf

[12] Singapore, Melbourne, Trondheim, Toronto are examples of metropolitan-scale systems.

[13] Privacy And Distance Based Charging For All Vehicles On All Roads. Stefan Eisses, Wiebren de Jonge and Vincent Habers: http://www.tipsystems.nl/files/Privacy_and_RUC_ITSLondon-doc.pdf

[14] National Surface Transportation Infrastructure Financing Commission: Paying Our Way, a New Framework for Transportation Finance, February 24, 2009: http://www.itif.org/index.php?id=227

[15] In the Netherlands for example all vehicles registered in the country will be covered by road pricing. There are, however, exemptions within this group: motorcycles and certain vehicles, such as emergency services. Exempted vehicles will not be fitted with an on-board unit.