THE JOURNAL OF NAVIGATION (2010), **63**, 51–59. © The Royal Institute of Navigation
doi:10.1017/S0373463309990300

Data on the Move – Privacy of Road Pricing

Bart Custers[1] and Albert Kuiper[2]

[1] (*Leiden University, Netherlands*)

[2] (*Capgemini Technology Services, Netherlands*)
(Email:bartcusters@planet.nl)

Privacy is an increasingly important aspect surrounding the introduction of road pricing in the Netherlands. Different systems for monitoring vehicles result in different consequences for privacy. This contribution describes the privacy aspects in the different scenarios used by the Dutch government. It is often suggested that privacy is a hindrance for road pricing, but if smart choices are made, this does not necessarily have to be the case. In this contribution, we suggest several concrete technological, legal and organizational (partial) solutions, that could be useful in implementing privacy-friendly road pricing.

KEY WORDS

1. road pricing. 2. privacy. 3. traffic monitoring. 4. onboard equipment.

1. INTRODUCTION.

The Dutch government has tried for many years to introduce road pricing, but these efforts have produced limited results due to political, organizational and technological reasons. Projects have been renamed and replanned many times.[1] The current program is focused on *OnBoard Equipment* (OBE) rather than *Automatic Number Plate Recognition* (ANPR). The viability of this programme remains unclear as the new plans for road pricing are still being developed and discussed. In preliminary studies, different scenarios have been suggested, but the advantages and disadvantages were not investigated as to what these scenarios offer regarding aspects including costs, security, enforcement and privacy.

Our contribution will focus on privacy, which is one of the aspects that is increasingly often the subject of public debate. The next section discusses the scenarios the government is considering as regards their privacy-friendliness. Since privacy is an interest that should be balanced against other interests, we will take other elements into account. It is sometimes suggested that privacy is a hindrance for effectiveness, enforcement, fraud control and customer friendliness. However, privacy can be well combined with these factors if smart choices are made. We suggest several concrete

[1] The current name is *Anders Betalen voor Mobiliteit* ('paying differently for mobility'). Previously referred to as *rekeningrijden* (*road pricing*) or *kilometerheffing* (*kilometer tax*).

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

Table 1. Four scenarios (thin, slim, smart and thick) with different functionality for the OBE and the Back Office.

	Thin	Slim	Smart	Thick
Collecting location data	OBE	OBE	OBE	OBE
Preparing location data	Back Office	OBE	OBE	OBE
Aggregating location data to road categories	Back Office	Back Office	OBE	OBE
Calculating road price	Back Office	Back Office	Back Office	OBE
Collecting the amounts due	Back Office	Back Office	Back Office	Back Office

technological, legal and organizational (partial) solutions that are useful in implementing privacy friendly road pricing. This contribution is based on Custers, (2008) which describes possible privacy issues of vehicle location data.

2. SCENARIOS.

Currently, the Dutch ministry of Transport, Public Works and Water Management is considering four scenarios, *Thin, Slim, Smart* and *Thick*. (Kilometer Pricing In The Netherlands, 2008). Each of these road pricing scenarios is based on determining a location by using a small device in the vehicle. This device is referred to as *OnBoard Equipment* (OBE) and is used to determine the amount due. In this respect, the Dutch approach differs to every other type of road pricing in the world. Other countries mainly use tollgates or Automatic Number Plate Recognition (ANPR), a system of gates with camera surveillance registering license plates. Until now, OBE has only been used experimentally for private traffic on a small scale.

In each scenario, road pricing is described as a process with several stages for determining the distances travelled and the amounts due. The scenarios differ in the level of autonomy in the OBE: how much information is processed in the OBE and whether the data is stored and analyzed on the OBE or in the central back office (see Table 1).

The route information is determined using satellite information. Using a Global Navigation Satellite System (GNSS – which includes both GPS and Galileo) signal, so-called *waypoints*, i.e., reference points, are determined. These waypoints are compared with roads on a map and the route is determined (see Figure 1). The digital map contains all information on pricing and the prices for the different road segments. In the example the trajectory on highway A28 is distinguished from the trajectories on the secondary roads. The information on the use of a road segment is added together per price category. After that, the categories are added together to a total amount. The pricing scheme may differ per type of vehicle; for instance, trucks and very polluting cars may pay more. When determining the road segment, the price table of the road is applied, which may include special objects (such as privately financed tunnels or roads) and may include different prices at different (congested) times. Charging will take place on a monthly basis, for instance: 250 km highway at 5 cent/km plus 1000 km secondary road at 2 cent/km plus 4 times a tunnel at €1 totals €36·50. A central back office takes care of the billing, fee collection and processing. Detailed information is available to distribute revenues to the parties involved, such as the central government, local governments, private road operators, etc.

The scenarios differ in the extent to which these stages are executed in the OBE or in a back office. A back office is a central administration unit, for instance, a government

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

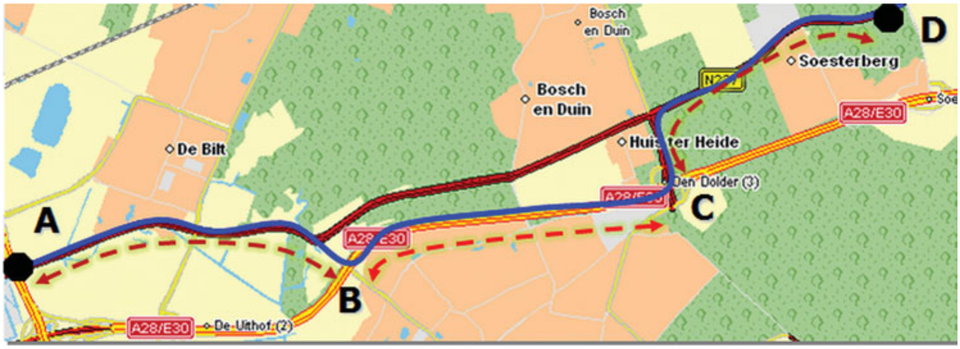

Figure 1. A route with two prices: using the highway or the secondary road. [2]

organization that processes the data and takes care of the billing process.[3] When more stages are executed in the OBE, this OBE has to be equipped with more functionality. The scenarios are indicated with the amount of functionality the OBE requires. The *Thin OBE* only collects data, the *Slim OBE* also prepares the data, the *Smart OBE* aggregates the route data for different road categories and the *Thick OBE* even calculates the entire pricing. Currently, the preference of the Dutch government is the Smart OBE.

2.1. *Scenario 1: Thin OBE.* The Thin OBE contains only the functionality to determine the location and an electronic identity. The waypoints, reference points for location determination, are transferred, preferably encrypted, together with the encrypted identity of the vehicle (the electronic license plate) to the central administration. At the central administration, the same card is used for all vehicles.[4] The information is extracted and processed just for pricing. The road segments are priced at the central administration using the price table and aggregated per category. The price tables are centrally stored and can easily be modified for all drivers at the same time.

2.2. *Scenario 2: Slim OBE.* The Slim OBE collects series of positions and aggregates these to a route using a digital route map. Instead of 25 separate waypoints on the route between The Hague and Amsterdam, the OBE concludes that highway A4 was used by a vehicle between a particular starting point and an endpoint. The amount of information to be transferred is reduced considerably in this approach. The route information is transferred to the central administration together with the encrypted identity of the vehicle (the electronic license plate). This is done at the end of each trip or periodically (monthly). The road segments are aggregated and priced

[2] Pricing the route: the distance is determined per category road and, in some cases, time. It is important to determine how many kilometers are driven on a highway (B-C), as this results in a different fee than use of a secondary road (A-B and C-D). The determination consists of a number of steps: determining the vehicle location (waypoints GNSS), determining the route and then the category of the road, deriving the distance per category, and accumulation per category. The four scenarios are different in the way and location of processing: in the vehicle or in the back office.

[3] In the Netherlands, both the *Belastingdienst* (The Dutch Tax and Customs Administration) and the *CJIB* (The Dutch Central Fine Collection Agency) are candidates for collecting the road pricing fees. Outsourcing to one or more private organizations is also being considered.

[4] However, this card may be dependent on target groups, for instance, for trucks. Heavy trucks only pay for primary roads within the treaty of the *Eurovignet*.

in the central administration. Since the Slim OBE is a commercial proposal, the exact technology is unknown.

2.3. *Scenario 3: Smart OBE.* In this OBE, the name refers to the 'smart' way of processing information. The concept is based on the location determination in the OBE, including the processing of a series of location determinations to a route. The smart OBE has a digital route map onboard. The road use is calculated per road category and this user information is transferred to the central administration together with the identity of the vehicle (the electronic license plate). The pricing and fee collection takes place at the central administration.

2.4. *Scenario 4: Thick OBE.* This OBE encompasses all functionality of the process, starting with the location determination, processing a series of location determinations to a route and calculating the price. For this purpose, the Thick OBE has a digital route map onboard. The map contains pricing data and for each trip the fee is determined by calculating the road segments per price category. The main difference between the Smart and the Thick OBE is that the Thick OBE has payment functionality. There is a 'digital wallet' onboard with a balance that can be charged. The driver has to check regularly whether the balance is sufficient or that the fees due are paid.

3. PRIVACY CONCERNS. The current privacy legislation in the Netherlands is laid down in the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*, WBP) and is based on a European Directive. Because of this directive at EU level, legislation in all EU member states is comparable to some extent. The main conditions for the legal processing of personal data are:

- *Transparency*: For each data subject, it must be clear who processes which information of a journey and for what purpose.
- *Legal basis*: For the processing of personal data, for instance, billing data, there has to be a legal basis. Consent of the data subject can constitute such a legal basis, but it could also be arranged as part of the new law regarding road pricing.
- *Focus on the purpose*: For each form of data collection, the purpose has to be clearly defined. Collecting data should be restrained and the data may not be used for other purposes such as marketing, travel advice or criminal investigation after some specified time.
- *Quality of the data*: Data should be sufficiently accurate and, when necessary, should be updated. Data that are not accurate or complete should be removed or corrected.
- *Rights of data subjects*: For data subjects there should be a possibility to inspect and amend (basic) data easily.
- *Security*: Adequate security should be ensured in order to prevent loss, unauthorized access or destruction of the data.

Since privacy is an interest that should be balanced against other interests, we will include the assessment of other interests. These main interests are:

- *Effectiveness*: The system must lead to a fair(er) pricing.
- *Costs*: The system may not be too expensive.
- *Enforcement*: The system must be sufficiently resistant to fraud.
- *User friendliness*: The user must experience the system as only a small hindrance or as no hindrance at all.

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

These considerations are taken into account as preconditions, i.e., they will not discussed here, unless they are not fulfilled. For the rest, it is assumed that all scenarios fulfill these conditions. The basic assumption is that detailed data are not accessible to third parties. However, there has to be access for data subjects (transparency, user friendliness), for enforcement (by a supervisory authority) or for refuting a fine. Regardless of where the data are, they must be accessible for these goals.

3.1. *Thin OBE Privacy Assessment.* All data are transferred to the central administration immediately after collection. The OBE serves as a black box; the user cannot see what is happening with his or her data. A possible solution for transparency and for user access and rectification is creating a system for users to log in to a personal website where their personal route data can be checked. By allowing a user easy access to check his or her personal data, the quality of the data can be improved. In this scenario, a lot of data is sent to the central administration. The level of detail of the collection of observations that is transferred creates both a privacy concern and a security concern. The privacy concern arises from the fact that a lot of information held together offers a more complete personal profile and thus offers more insight in the lives of data subjects. A solution for this is to encrypt the data and to provide employees of the back office only access to those data they need to know for their tasks (so-called role-based access). The security concern arises from the fact that a lot of information together creates value and therefore becomes more attractive for hackers, for instance, for committing identity fraud. Cryptography and compartmentalization (subdividing data to ensure a successful hacker only gains access to a meaningless part of the data) may be helpful tools to prevent this.

3.2. *Slim OBE Privacy Assessment.* In most respects, the Slim OBE hardly differs from the Thin OBE. One important difference, however, is that much less data are sent to the back office. This reduces the privacy and security concerns. Nevertheless, for enforcement the registration of waypoints needs to be stored in the OBE to enable comparison checks with the central administration. For the Thin OBE such checks are also desirable, but less necessary because any interpretation errors take place at the central administration (and can be checked there) and not in the Slim OBE.

3.3. *Smart OBE Privacy Assessment.* From a privacy and security perspective, this scenario is favourable for several reasons. First, the location data are not centrally available. This prevents building integral personal profiles of someone's whereabouts. (Data in the OBE has to be accessible externally for enforcement purposes, but accessibility per OBE is a decentralized solution.) In addition, using information for other purposes, such as browsing the data for patterns is impossible. Obviously, this may also be a disadvantage, since this may hinder the realization of particular policy goals, including, for instance, traffic jam predictions, information for road maintenance organizations, assigned quotas regarding pollution at particular locations or large scale criminal investigations. Customer friendliness may also decrease, since errors cannot be rectified by the central administration straightaway. All data are in the vehicle, which means that a visit to a service location may be required for the vehicle. In this scenario, the introduction of a Multi Service Provider (MSP) model is considered. In such a model, private operators offer OBEs next to the back office functionality. When each MSP uses its own technological standards for the digital maps and algorithms for determining routes (often a patented concept), this may lead to mutual differences. In exceptional cases, this might result in (slightly) different fees for different OBEs on the same route.

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

3.4. *Thick OBE Privacy Assessment.* Just like the Smart OBE, the Thick OBE does not provide central access to vehicle location data, with the same consequences for the privacy, security, effectiveness and enforcement. The Thick OBE has payment functionality onboard and this may provide more of sense of privacy for the user, as he or she may check all payments directly. Obviously, this assumes that the OBE is designed in such a way that a user may communicate with it, for instance by adding a screen and some buttons. There is an issue with enforcement, however, as this OBE is more susceptible to fraud. Until now, providers of mobile telephony have never added calculation and payment functionality on their cell phones because security is difficult to arrange. For a more detailed discussion, see Custers, (2004), Borking & Raab, (2001).

4. SOLUTIONS.

It is clear that all scenarios have shortcomings on one or several points with regard to privacy and security. However, there are several (partial) solutions that may contribute to better fulfilment of the abovementioned conditions regarding privacy and security. These solutions are applicable in all scenarios described to some extent. The list below is not complete, but merely intended to provide an idea of possible instruments for privacy-friendly solutions.

4.1. *Technological Solutions.*

4.1.1. *Anonymization.* One of the most important privacy enhancing technologies is the anonymization of data. The data of a Mister X are much less privacy sensitive than the data of Queen Elizabeth. Many of the purposes of road pricing, including reduction of traffic jams, can be realized with anonymous data. Pricing, however, is never anonymous as the bills have to be sent to individuals. Nevertheless, even with pricing it is possible to anonymize several stages of the process. The Personal Data Protection Act is not applicable to anonymous data. This creates more freedom to collect and process data, but there is less legal protection for individuals.

4.1.2. *Encryption.* The use of cryptography prevents easy data leakage. Anyone obtaining unauthorized physical access to data files will only see garbled text. Encryption also reduces the harm of data leakage when employees lose CD or USB memory drives.

4.1.3. *Secret Sharing.* Based on encryption, secret sharing is a way of 'dividing' the secret key that provides access to data among several people. This does not involve dividing the key itself, but pieces of information which lead to access to data. For instance, PIN code 8706 is not divided in half, one user receiving 87 and the other 06. This system works by giving one user number 2145 and the other 6561 which therefore does not reveal the whole key. In this way, only two people together may combine their keys to gain access to the data. This may also be transformed into other forms of access, like 'three out of four people' or 'two police officers in combination with either the public prosecutor or the data subject.' When a key is divided between a data controller and a data subject, this offers additional possibilities for transparency, inspection and correction. For instance, arrangements can be made that a data subject always has to be involved in any change in his or her data. Sharing a key among several data controllers may offer additional security against employees who want to look into the files of their neighbours or celebrities.

4.1.4. *Role-Based Access.* This solution is based on not providing users access to all data in the database, but only to data that are necessary for performing specific

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

tasks. This principle is usually referred to as *need-to-know*. An employee assigned with billing needs to know the number of kilometres travelled, but not necessarily all of the locations where the vehicle has been. A data subject may have access to his or her own data (for instance, by using a personal log-in), but not access to that of a neighbour.

4.2. *Legal Solutions.*

4.2.1. *Explicit Legal Basis.* Currently, there is a lack of clarity in laws and regulations concerning particular points on when data may be collected and processed. There are several ways of providing more clarity in these matters. Once it is clear which data are required, there has to be an unquestionable legal basis. The informed consent of the data subject may constitute such a legal basis, but this is not very likely to happen unless data subjects have some financial incentive (for instance, when the new system of road pricing turns out to be cheaper than the current road and car tax system). The new Road Pricing Act has to indicate what data are collected and processed, by whom, and how this happens and which storage times are applicable. Furthermore, there is the possibility of drafting covenants between the organizations involved to make (more) explicit which data are exchanged and for what purpose.

4.2.2. *Extending Privacy Protection.* For some parts of the process it is not clear whether the data that is being processed is personal data and whether the Personal Data Protection Act is accordingly applicable. For instance, this act does not apply to anonymous data and number plate data is only personal data when it is possible to link it to an identifiable or identified individual. As a result, for those involved part of the regular legal protection is lacking since only when the Personal Data Protection Act is applicable are there rights for inspection and corrections. By clearly indicating and, at some points, extending the legal protection it is likely that public support will increase. This problem can be solved with technology by using an encrypted electronic license plate at the source and in transactions.

4.2.3. *Strong Fraud Enforcement.* The collection of road pricing fees amounts to approximately six billion Euros each year in the Netherlands. This amount does not include any costs regarding the introduction of the new system. With revenues this size, fraud is likely to crop up. Enforcement is primarily carried out through observations (e.g., camera surveillance, Automatic Number Plate Recognition) that are compared with the route data, either real-time or afterwards. Such comparisons may be harmful to privacy, as the accounts have to be checked. The Tax Authorities will regard such registration equipment as means for accounting. When fraud is suspected, further investigation will follow. In the case of a criminal investigation (which is not just a check!) the data controller will have to provide access to data. Obviously, the question then is whether cooperation is mandatory, i.e., who is allowed to access the data and when. The Tax Authorities require no additional powers because the current legislation provides these. For other investigation agencies, including the police, this could be different. The most likely approach in these cases is that permission of the public prosecutor or the examining judge will be required, as he is able to balance the interests of privacy on the one hand and criminal investigation on the other hand. However, a clear and unambiguous procedure still needs to be drafted for this.

4.2.4. *Strong Privacy Enforcement.* Privacy needs to be enforced as well. Currently, this is the Data Protection Authority's (*College Bescherming Persoonsgegevens*, CBP) responsibility. Since this supervision has not been working well, the CBP

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

drafted new policies for stronger enforcement in their 2008 plan. It is expected that this new approach will strengthen the position of the CBP, so that it is more comparable to supervisory authorities in other sectors. Sanctions such as fines and administrative coercion are possible tools the CBP can use for this.

4.2.5. *Inspection and Correction Tools.* For data subjects it should be clear who is collecting what information and for which purpose. This transparency can be provided by offering inspection tools such as, for example, a website that a user can log into or by contacting a helpdesk. When data are incorrect or incomplete, correction tools may be useful to improve data quality. Obviously, checks are needed to prevent fraud in any requested changes. Inspection and correction tools are not only mandatory, they may also contribute to support among citizens. As long complaint procedures may be very costly and useless it is recommended to introduce swift settlements on any disagreements, .

4.3. *Organizational Solutions.*

4.3.1. *Informing the Public.* Most of the abovementioned technological and legal solutions will only be useful when citizens are sufficiently aware of possible privacy issues that may occur. Information campaigns may concern both data subjects and data controllers. (See Custers, 2008). For both groups it should be clear what the rules are and what the rights and duties are in case these rules are violated. A data subject can only file a complaint when he is aware by whom his data is processed (transparency) and whom he may hold accountable (responsibility). This requires data subjects to have a certain amount of knowledge and awareness and, as such, it is reasonable that data controllers clearly explain how they operate and what the parameters for filing complaints are.

4.3.2. *Inspection and Correction Tools.* Inspection and Correction Tools were mentioned above as legal solutions, but they also have an organizational component because they require the introduction of additional procedures regarding inspection and correction. These are not mentioned in any detail in the current plans for road pricing in the Netherlands. Furthermore, in cases of rectification, there has to be a check to see which data are correct. Also there should be an organizational culture of transparency that does not immediately assume that information systems are always right. Employees have to be aware of the possibility that information on their computer screens is not always reliable. (See Vedder and Wachbroit, 2003).

5. CONCLUSIONS. The question to be answered is which scenario is preferred in light of the considerations above. All scenarios are possible and reasonable when a selection of the abovementioned (partial) solutions are combined and applied. Because of their decentralized approach, the Smart and the Thick OBE are preferred from a privacy perspective. The Slim OBE is preferable above the Thin OBE, as it collects and processes less data. When the solutions mentioned above for ensuring more privacy are implemented, the balance may shift towards the two 'thin' versions in which a central back office provides more ease of use. Even though vehicle location data are available in the central back office for particular processes in this case, a complete picture of the data subject is not available.

Regardless of which scenario is chosen, it is recommended to integrate the suggested (partial) solutions previously mentioned in the chosen scenario. Although not all of the solutions are strictly necessary, they offer the best guarantee for ensuring

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press

maximum privacy. In this way, data can be prevented from being moved to places unknown.

REFERENCES

Borking, J. J., and Raab, C. D. (2001). Laws, PETs and other Technologies for Privacy Protection, *Journal of Information, Law & Technology* (*JILT*), Vol. 1, No. 1.

Custers, B. H. M. (2004). *The Power of Knowledge*, Tilburg: Wolf Legal Publishing.

Custers, B. H. M. (2008) *Privacy Issues of Traffic Monitoring*. In: Hasani Mohd Ali and Aishah Bidin (eds.) *Abstracts & Proceedings*, 3rd Conference on Law & Technology (CLT3, 2008), Kuala Lumpur, Malaysia, p. 85–94.

Kilometer Pricing in the Netherlands (KMP), Information Update, Presentation of the Ministry of Transport, Public Works and Water Management, 15th April 2008.

Vedder, A. H., and Wachbroit, R. (2003). Reliability of Information on the Internet: some distinctions, *Ethics and Information Technology*, 2003, **5**, 211–215.

https://doi.org/10.1017/S0373463309990300 Published online by Cambridge University Press