

KEEPING BIG BROTHER OFF THE ROAD

National road pricing schemes aren't necessarily incompatible with the driver's right to privacy


By Robert Harle and Alastair Beresford

AS EVERY UK CAR owner knows, the country has the most congested roads in Europe; the M25 alone sees an average of 258,000 vehicles per day. What's more, it's going to get worse. Annual vehicle kilometres have grown near-linearly since records began in 1955, and increased by an estimated 8.2 billion vehicle kilometres in 2004. If current trends continue, traffic levels will double over the next 40 years and the UK will face gridlock in its towns and cities.

Congestion charging is widely seen as the most effective way of addressing this problem. The London congestion charge, introduced in 2003, has resulted in a 33% drop in traffic entering central London and a corresponding 10.4% increase in average road speed during evening peak hours. Spurred on by these achievements, Transport for London (TfL) is seeking to expand the charging zone, while the Department for Transport (DfT) has actively been investigating national road pricing schemes.

The potential benefits are considerable, but the technical challenges involved in the provision of a large-scale charging scheme are immense. How do we know where every car goes? How do we charge the drivers? How does enforcement work? And can we reap the benefits





without risking the Orwellian nightmare of a world in which a 'big brother' central authority tracks and collates the movements of every vehicle?

EXISTING SOLUTIONS

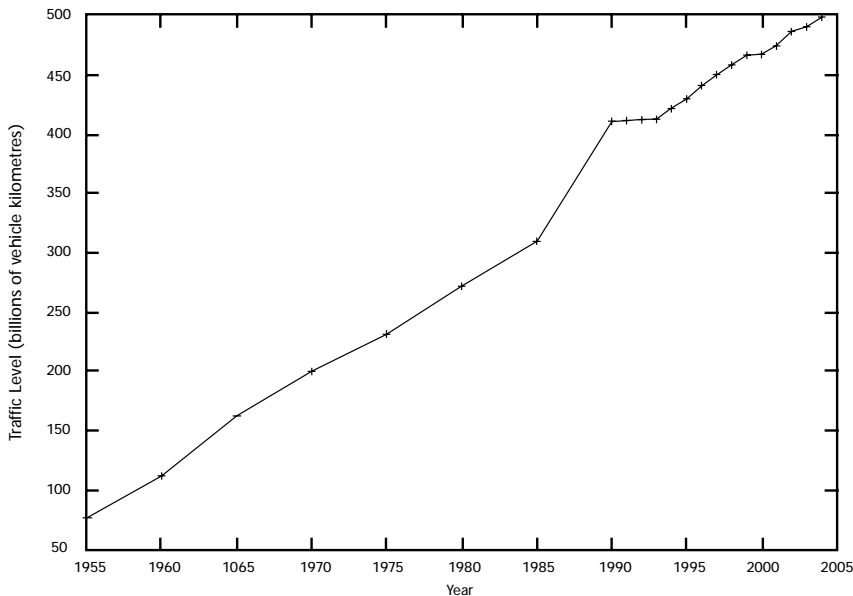
The key to any national road pricing scheme is the ability to charge by time, distance and place. Technologies currently being considered as a means of satisfying these requirements include toll booths, radio tags, GPS and automatic number plate recognition (ANPR). The London congestion charge uses ANPR, identifying and logging each vehicle that enters central London. However, the infrastructure is expensive and unwieldy, and TfL recognises that it cannot easily be extended to operate on a national scale.

Perhaps the biggest problem faced by designers of new charging systems is that, currently, ANPR is the only practical way to remotely identify a UK vehicle. Radio tags can be used to identify a specific vehicle, but there is still a need for a secondary enforcement mechanism, something like a physical barrier to catch fare-dodgers. Unfortunately, such barriers tend to impede the flow of traffic, risking additional congestion. ANPR can be used to capture license plates without affecting traffic flows, although this reduces the probability of capturing a fare-dodger to around 90%.

A 'black box' in every vehicle, tracking when and where the vehicle goes, has been proposed as an alternative to ANPR, and motoring insurance companies have pioneered the use of these technologies to enable pay-as-you-drive policies. However, there are problems in applying this approach to congestion charging: the information has to be transferred to the charging authority; and there is no obvious way to counteract the driver who simply disconnects the GPS antenna. Unfortunately, with all current technologies, an expensive network of fixed cameras would appear to be the only reliable way to identify fraudsters.

PRIVACY CONCERNS

All existing solutions concentrate on meeting the charging authority's requirements, while often failing to recognise the →



Above: Onward and upwards – the UK's escalating traffic levels

privacy of individuals. Many in the transport industry acknowledge the inherent risks to privacy in current proposals, but simply regard the potential threat as a 'necessary evil'. Privacy is a right enshrined in UK law, and is the exclusive concern of Article 8 of the 1998 Human Rights Act.

The DfT's Feasibility Study of Road Pricing in the UK (see 'To probe further' panel, opposite) concludes that the Human Rights Act "does not... prevent or impede the collection of the data needed for road charging" provided that "charging authorities... ensure that they only collected data on vehicle movements that was needed to administer and enforce". However, in the same document, the DfT notes that a national distance-charging scheme would "involve collecting detailed data on all vehicle movements". Of course it would be possible to have procedures in place to delete centralised information on honest, paying individuals. However, in practice, the temptation to reuse the data or infrastructure, once it has been created, is likely to be too great to resist.

These issues are not exclusive to congestion charging schemes; rather they are systemic in many technological developments, where privacy is considered as an afterthought or not at all. As engineers, we need to learn to think differently, and build suitable privacy measures into the hearts of our designs. With congestion charging, as with most systems, there is another way.

DEVELOPING ALTERNATIVE DESIGNS

Enforcement is a valid concern in the design of congestion charging systems, but this does not necessarily require the centralised collection of all

vehicle movements. An alternative solution is to keep information on the cars themselves, with vehicles validating congestion charge payments with each other. This approach would reduce fixed infrastructure requirements, while the associated on-car equipment could be checked as part of regular vehicle maintenance and MoT testing. Four additional devices would be required on each vehicle: a cheap camera, a small radio transceiver, an embedded computer and a positioning system. These components could be built into an 'intelligent' number plate that could be retrofitted to existing vehicles.

In operation, the vehicles would use the radio interface to communicate with the central charging authority, purchasing congestion charge tickets and downloading current prices and charging zones into a local database. Communication with other vehicles is also by radio. As the vehicle moves, the positioning system estimates the instantaneous location, which, used in combination with the local database, allows the computer to determine the current charging zone. The computer also analyses the video stream from the camera and uses ANPR to identify any vehicles in front of it. If ANPR successfully identifies a vehicle, the computer uses the radio channel to request the electronic ticket from the identified vehicle; thereby verifying payment. If verification fails, the image is stored by the car, until communication with the central authority becomes possible.

In this scheme, enforcement is achieved primarily by other vehicles, and not the central authority. Cars that present a valid electronic ticket will not have their



movements transmitted to a central database. Inevitably, reporting of fare-dodgers by any one car will not be completely reliable, as some ANPR and radio errors are unavoidable. However a vehicle travelling any reasonable distance will normally be seen by many vehicles and therefore fare-dodgers will usually be caught. In the scenario when there are only a few other vehicles around, a congestion charge is unwarranted.

It is possible that a 'rogue' vehicle may attempt to report every vehicle to the central authority, through error or malice. This, however, is relatively easy to detect, and in any case, a driver with a genuine electronic receipt can always prove payment later. Drivers may attempt to break the system by disconnecting system components, such as the GPS antenna. However this is unwise, since the vehicle is then very likely to be captured by other vehicles and reported. In practice, it is in the driver's interest to maintain a functioning congestion charging unit.

The system can charge by time and place, but distance-based charging will require adaptation. One possibility is for each vehicle to record the mileage it observes other vehicles doing and report this to the charging authority. At the end of a charging period each car must report the total distance covered, which must be greater than, or equal to, the sum of reports to the authority from other vehicles. If a vehicle repeatedly reports a false mileage the central authority can issue a penalty notice.

BENEFITS

The overall result of this design is that drivers achieve privacy only by paying the congestion charge, and the balance of probability says they will be caught if they

TO PROBE FURTHER

ROAD TRAFFIC STATISTICS: 2004, DFT

www.dft.gov.uk/stellent/groups/dft_transstats/documents/page/dft_transstats_038885.hcsp

'PAYING FOR ROAD USE', COMMISSION FOR INTEGRATED TRANSPORT

www.cfit.gov.uk/reports/pfru

LONDON TRAVEL REPORT 2004, TFL,

www.tfl.gov.uk/tfl/ltr2004/index.shtml

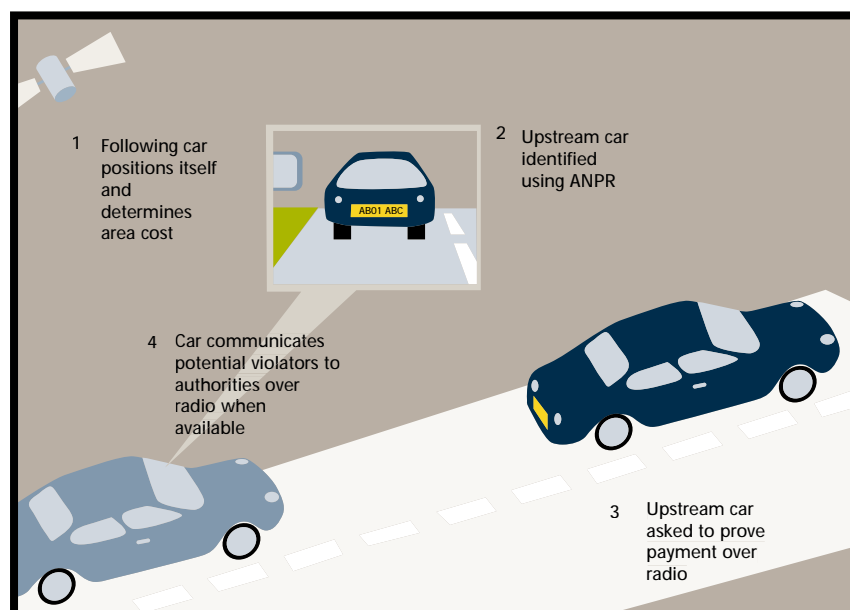
'FEASIBILITY STUDY OF ROAD PRICING IN THE UK', DFT,

www.dft.gov.uk/stellent/groups/dft_roads/documents/page/dft_roads_029788.hcsp

'LONDON CONGESTION CHARGING TECHNOLOGY TRIALS', TFL,

www.tfl.gov.uk/tfl/cc_london/cc_publications-library.shtml#trials

Below: A working scenario



don't. We estimate the probability of successfully avoiding payment should be much lower than the London congestion scheme, where TfL estimate that 10% of cars are not correctly identified. The scheme should also be relatively cheap to deploy. Many modern cars are already equipped with GPS; suitable computer performance and radio interfaces are likely to be available in many models in the near future. It is possible that a charging scheme similar to the one proposed could be introduced in many vehicles through a camera installation and software upgrade.

Attaining privacy in large-scale systems is not only possible, but can be surprisingly compatible with other design goals. However, privacy is a difficult design criterion to get right. It requires attention throughout the product development cycle, from the conception and early development of a product, right through to deployment and maintenance. As engineers, we should be thinking more about privacy in the systems we design for tomorrow. ■

Robert Harle and Alastair Beresford are Research Associates at the University of Cambridge Computer Laboratory. They can be contacted at Robert.Harle@cl.cam.ac.uk and Alastair.Beresford@cl.cam.ac.uk.