COMMENTS ON THE "PAY AS YOU DRIVE" PROPOSAL

ANDREW J. BLUMBERG (STANFORD UNIVERSITY), LEE TIEN (ELECTRONIC FRONTIER FOUNDATION), AND PETER ECKERSLEY (ELECTRONIC FRONTIER FOUNDATION)

1. Comments

We wish to register significant privacy concerns about the "Pay as you drive" (PAYD) insurance premium pricing proposal that the California Department of Insurance is considering. In itself, the proposed shift to fine-grained pricing dependent on the precise number of miles a car is driven in a given billing period is an excellent one. We expect that this will allow insurance companies to offer targeted incentives to reduce overall vehicle usage across a wide range of driving patterns.

However, we strongly object to the threats to customer privacy associated with many of the proposed technical implementations of PAYD. Insurance companies seem to be interested in pursuing this kind of scheme via a "black-box" recording device placed in customers' cars; this device would contain a radio transmitter and would transmit realtime or near-realtime signals regarding positional data (via GPS) and potentially other sorts of data about car motion (acceleration, braking, and so forth). For instance, Progressive has already begun a pilot program in which they offer rebates to drivers who allow such a device to be placed in their car.

Such a device would almost certainly support radical violations of the "locational privacy" of the drivers; it would form the basis of a pervasive surveillance and tracking infrastructure. Beyond the explicit objections to such privacy violation, from a pragmatic standpoint we expect that very strong and broad opposition would be mobilized to protest such a device, and this might threaten the adoption of the PAYD insurance scheme. Since the PAYD premium scheme can be implemented without these devices, we can only regard the discussion of them in this context as subterfuge designed to get such devices into cars (via potentially coercive pricing policies) and acclimate drivers to the presence of pervasive monitoring.

To summarize our position, while we do not object to PAYD pricing implemented with strong privacy safeguards, we oppose permitting any sort of "black-box" or GPS monitoring device-based implementation of this scheme and recommend explicitly prohibiting it in the revised PAYD regulations:

- The risks of abuse and the threat to consumer privacy is enormous, and carefully designing protections and policies to address this is a tremendous and labor-intensive project.
- Such devices are *completely unnecessary* to implement the full scope of PAYD pricing policies, and are useful only for future applications, which raise classic privacy issues about mission creep and the use of data for a purpose other than that for which it was originally collected.
- The best protection is not to collect the data in the first place, particularly when the data isn't needed to carry out the desired application.
- Intense public opposition will likely be generated once the scope of such monitoring devices is known, which could threaten the PAYD policy adoption.

1.1. **The threat to locational privacy.** The prototypical device which is going to be used for this scenario monitors acceleration and car location. The uncontrolled adoption of such devices is potentially extremely dangerous, as they will permit very strong violations of the "locational privacy" of the driver. Locational privacy is the ability of an individual to move in public space with the reasonable expectation that their location will not be systematically and secretly recorded for later use. Note that our concern is not with the security of the transmission channel; even assuming that the signal from the device to the insurance company is encrypted, there are very real perils associated with building infrastructure to allow companies to maintain extensive tracking databases of the motions of customers.

The systems discussed above have the potential to strip away locational privacy from individuals, making it possible for others to ask (and answer) the following sorts of questions by consulting the location databases:

Date: June 18, 2008.

- Did you go to an anti-war rally on Tuesday?
- A small meeting to plan the rally the week before?
- At the house of one "Bob Jackson"?
- Did you walk into an abortion clinic?
- Did you see an AIDS counselor?
- Have you been checking into a motel at lunchtime?
- Why was your secretary with you?
- Did you and your VP for sales meet with ACME Ltd on Monday?
- Which church do you attend? Which mosque? Which gay bars?
- Who is my ex-girlfriend going to dinner with?

Of course, when you leave your home you sacrifice some privacy. Someone might see you enter the clinic on Market Street, or notice that you and your secretary left the Hilton Gardens Inn together. Even in the world of ten years ago, all of this information could be acquired, with enough time and effort. But obtaining this information used to be expensive. It is the transformation to a regime in which this information is recorded pervasively, silently, and cheaply that we're worried about.

Our concerns are manifold. For one thing, the "legitimate" insurance applications of such data is potentially very worrisome. Some of the possible applications might include:

- Higher premiums for people who drive and park in neighborhoods with high vehicle theft and crime rates, e.g. impoverished and/or immigrant neighborhoods.
- Higher premiums for people who drive at night or other unusual times (say, for work reasons).
- Higher premiums for drivers with behavioral choices that correlate with higher accident rates, potentially in the absence of any reasonable causation or fault.

And one could easily imagine "linkage" to other kinds of insurance decisions: your health insurance provider might be very interested in exploiting data about your behavior and whereabouts to determine if you are living an "unhealthy" lifestyle and thus should be assessed higher premiums.

Furthermore, the databases maintained by the insurance companies will of necessity be secret and the algorithms used to determine cost profiles will likely be proprietary. This lack of "sunshine" permits abuses both because it is difficult to appeal problems in secret databases (the well-known difficulties associated with appealing mistakes in credit profiles provide instructive examples in this regard) and because it makes it difficult to detect when there are explicitly discriminatory pricing policies in use. Building infrastructure for massive "lifestyle redlining" seems like a bad idea.

Beyond the issues with use by the insurance companies, there are also terrible potential problems associated with the long-term storage of such data. Such data could easily be requested by various other branches of the government (e.g. law enforcement), as we have seen with search engine data. Furthermore, civil subpoenas might make such data available in court — this is already the case for the automated tolling data recorded by EZpass.

We are extremely suspicious of any promises of privacy on the part of the insurance companies — the problems with identity theft already make clear how fraught with danger this issue is, and the insurance companies have much less fiscal incentive to be careful than the credit card companies. Enforcing regulations designed to protect consumer privacy is very difficult; the best protection is not to collect the data in the first place, particularly when the data *isn't needed to carry out the desired application.*

The "Pay as you drive" protocols as discussed in the brief depend only on odometer readings; there is simply no reason under the current proposed tolling structures to have any sort of tracking device inserted into customer vehicles. The insurance companies are already guaranteed by law the ability to inspect odometers to verify mileage reporting. Voluntary reporting coupled with random spot checks and sizeable penalties for deception would easily accommodate PAYD (e.g. forfeiture of coverage for cars involved in claims where the odometer readings are determined to be at variance with the self-reporting).

1.2. **Summary.** The "Pay as you drive" insurance premium structure is an innovative and exciting proposal. But any implementations of it which depend on installing "black box" surveillance devices in customers' cars pose an unacceptable threat to locational privacy. Building a massive tracking infrastructure in a legal environment in which there are weak restrictions on the use of such data is irresponsible. Furthermore, it seems highly likely that if permitted the devices will be promoted via coercive means; premium subsidies for drivers who allow the devices are the same as a surcharge on customers who don't sacrifice their privacy. It

is totally unacceptable for a service mandated by law to coerce consumers into sacrificing their privacy in an ill-specified way. No one should be induced to sell their right to privacy.

Finally, should the Department of Insurance decide at a later date that more sophisticated behavioral monitoring is appropriate or that there really are compelling reasons to permit some kind of remote monitoring of odometer readings for PAYD, there are cryptographic protocols which allow this to be done in a way which preserves locational privacy and *does not involve tracking the motions of the driver*. However, we believe that discussion of such algorithms is premature at this date given the fact that it is so straightforward to use odometer readings for PAYD as proposed.

Andrew J. Blumberg, Postdoctoral fellow, Department of Mathematics, Stanford University, Stanford, CA 94305

E-mail address: blumberg@math.stanford.edu

Lee Tien, Senior Staff Attorney, Electronic Frontier Foundation, 454 Shotwell St., San Francisco, CA 94110

E-mail address: tien@eff.org

Peter Eckersley, Staff Technologist, Electronic Frontier Foundation, 454 Shotwell St., San Francisco, CA 94110

E-mail address: pde@eff.org