



# Pay-as-you-drive application

Carmela Troncoso (KU Leuven-  
Cosic/IBBT)

Joint eSecurity WG / Article 29 WG meeting  
14<sup>th</sup> October 2009



# Pay-As-You-Drive: the concept

---

- } Flat fees are not fair for everyone
  
- } Users should pay depending on their use of the car and roads:
  - } Long drives, high density roads, rush hours: higher fee
  
  - } Sporadic use, second vehicle for weekends, young drivers with small salary: smaller fee
  
- } **Applicability:**
  - } Vehicle insurance
  - } Road Charging (taxes)
  
- } This presentation is centred on the insurance case (see Stefan Motte's presentation on road charging)

# Pay-As-You-Drive: pros

---

- } Fair fees
  - } For customer and companies
- } Customer can “choose” his premium
- } Social benefit
  - } less use of cars, responsible driving, less accidents, improve road mobility...
- } Environmental benefit
- } Business advantage position
  - } Data mining
  - } Additional services (LBS, targeted advertising,...)

# PAYD: straightforward implementation

- } Black box in car continuously collects data
- } Use GPS for location
- } Use GSM for transmission (continuously or not)



Octo telematics (3rd party)



Progressive Insurance



MAPFRE



Uniq Group



STOK (3rd party)



Hollard (Mobile Data)



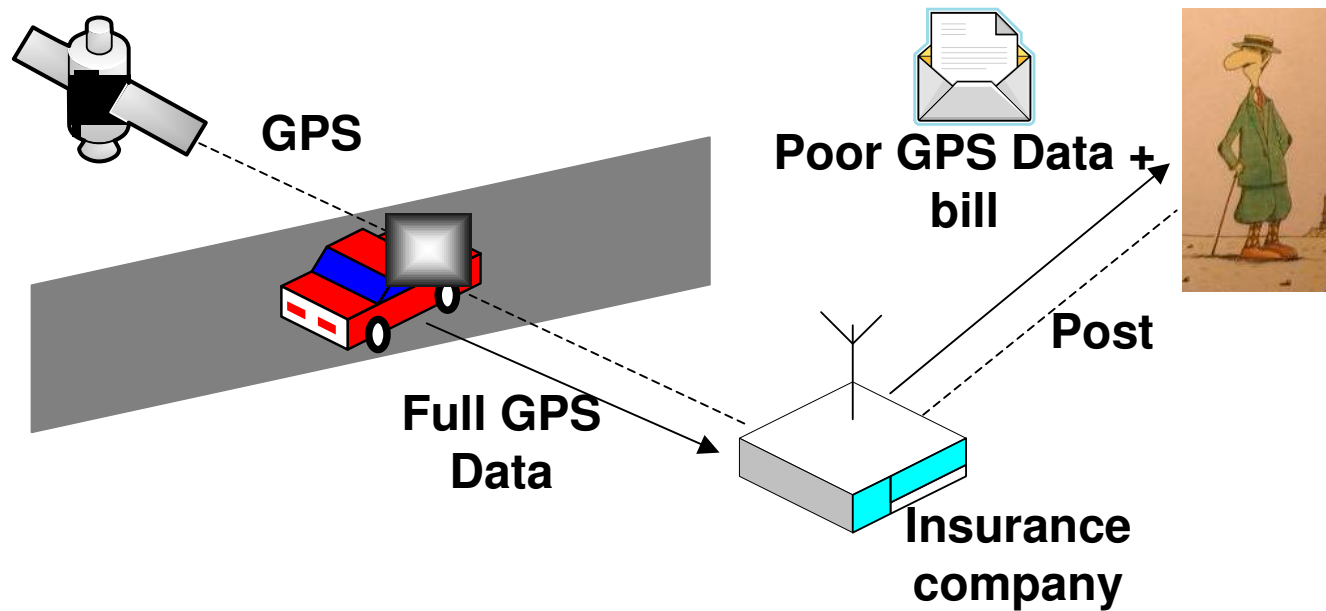
AVIVA



iPAYD (3rd party)

# PAYD: straightforward implementation (II)

} Black box + GPS + (third party) + transmit



# Pay-As-You-Drive: cons

- } Location data is highly sensitive:
  - } Inferences about driver [Iqbal 07]: personal, government, businesses
  - } Anonymization **very** difficult
    - } What is anonymity?
      - } property of an individual of not being identifiable within an anonymity set
      - } probabilistic concept
      - } cryptographic protocols (identity management) anonymity achievable but...
    - } Traffic analysis -> anonymity extremely hard
      - } Tracking techniques [Gruteser and Hoh 05]
        - } Exploit spatio-temporal relations
      - } Work/home is enough for re-identification [Golle and Partridge 09]
        - } approximate locations of an individual's home and workplace can be deduced from a location trace (median size of the individual's anonymity set in the U.S. working population is 1)

# Pay-As-You-Drive: cons

- } Data security is hard to achieve:
  - } Even if a system is Data Protection compliant...
    - } Accidental leaks (Toyota, Norwich Union)
    - } Insider attacks (Greek Mobile Phone Scandal)
    - } Outsider attacks (10, 000 Hotmail passwords released by hacker – 6th Oct)
  - } ... and once data is leaked, there is no control over it
    - } Harvard Student database on BitTorrent 2008 (name, Social Security number, date of birth, address, e-mail address, phone numbers, ...)
  - } How long should it be kept?
    - } Data retention
  - } Liability
    - } What if data is lost/tampered?
  - } Need for certification

# Pay-As-You-Drive: cons

- } Legal issues:
  - } Data subject:
    - } Car vs driver
    - } Children vs parents
    - } Employer vs employee
  - } Data Controller:
    - } Box vs Insurance company
    - } Telecom provider
  - } Data minimization and proportionality
    - } GPS data reveal far too much information (e.g., speed, inferences)
  - } Secondary use of data (collides with purpose of the service)
    - } Back to anonymization problem ...

# Pay-As-You-Drive: cons

- } Third parties issues:
  - } False sense of privacy
    - } AVIVA in France, MAPFRE in Spain, ...
  
- } Aggregation of data
  - } Larger databases (Octo Telematics: 30 insurance companies / 858.775 users)
  
- } Data security
  - } More entities involved make securing data even more difficult
  - } Data controller?

# Conclusions

---

- } PAYD has many advantages but its implementation may have catastrophic privacy consequences
  - } Sensitivity of location data
    - Difficult to anonymize
    - Inferences, combination with other sources of data
  - } Data security
    - Leakage can always happen
  - } Legal issues
    - Actors difficult to distinguish
  - } Third parties
    - False sense of privacy
  
- } Solutions
  - } Computation in the box (PriPAYD [Troncoso et al 07])
    - Working prototype
  
  - } Half-way solutions
    - Ongoing work with NXP within NextGen ITS IBBT project

# Thanks for your attention!

---

## QUESTIONS?

[Carmela.Troncoso@esat.kuleuven.be](mailto:Carmela.Troncoso@esat.kuleuven.be)

### } Further reading:

- } C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, "PriPAYD: Privacy Friendly Pay-As-You-Drive Insurance," In Proceedings of the 6th ACM workshop on Privacy in the electronic society (WPES 2007), T. Yu (ed.), ACM, pp. 99-107, 2007
  - } Extended version under submission
- } J. Balasch and I. Verbauwhede, "An Embedded Platform for Privacy-Friendly Road Charging Applications." Under Submission to Design, Automation and Test in Europe (DATE 2010), 2009.
  - } Demo needs to be improved
- } A. Rial, J. Balasch, C. Troncoso, B. Preneel, I. Verbauwhede, "Optimistic Payment and its Application to Privacy-Preserving Electronic Traffic Pricing" Ongoing work.