



Privacy Enhancing Technologies for Mobile Services

Andrew Matthews
Cambridge Wireless – Location SIG
23rd March 2011

Nokia World 2010 talk– Sir Tim Berners-Lee

- Internet founder Sir Tim Berners-Lee details four concerns about future of the mobile Web

15th September 2010

- **Privacy**

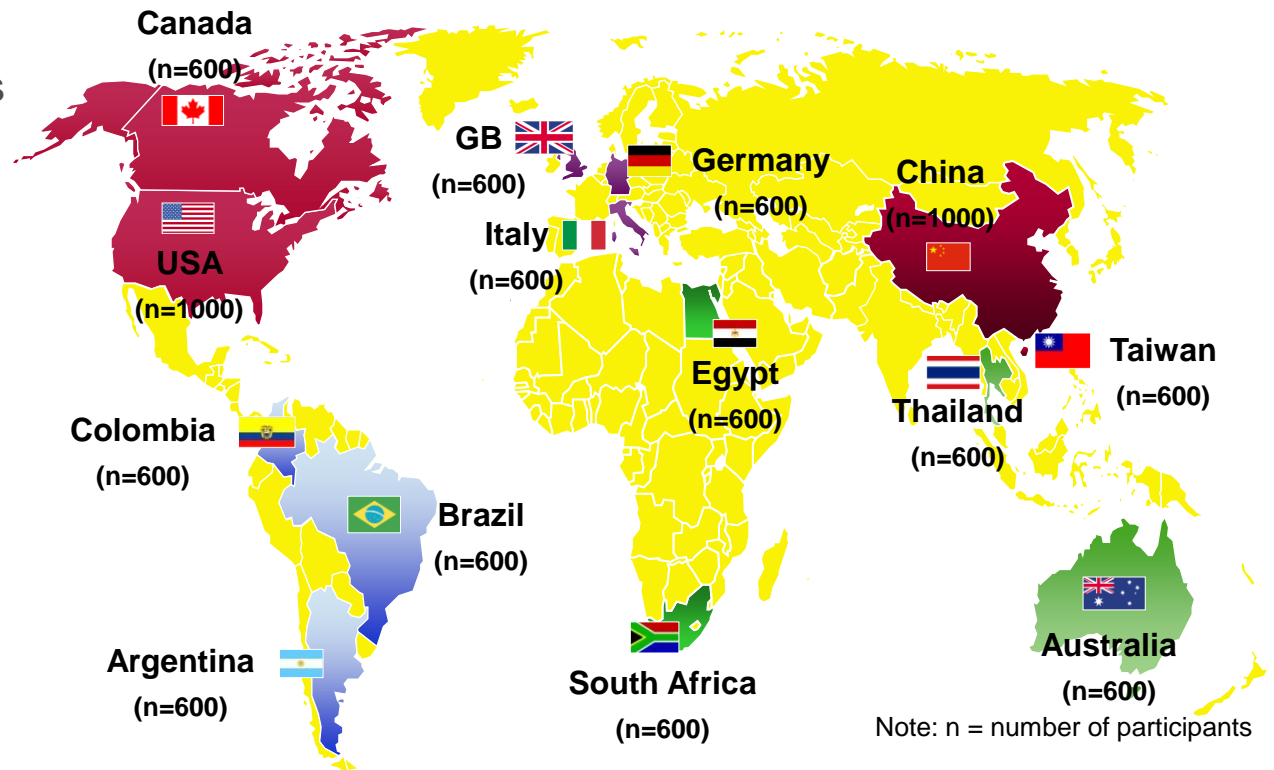
The challenge of **privacy** is one many companies, both mobile and otherwise, have been dealing with in recent months. However, on mobile phones, the **problem** that has not been worked out yet **is how to allow a user to share their location while still making it easy for them to understand when they're sharing critical information, how much control they have over that information and who can access that data.**

The challenge is how to do this without getting in the way of user's experience.

- This relates to many aspects including:
 - “Apps” and “Freemium” business models
 - Small screens & (limited) data contracts

Privacy in a mobile context

- Nokia Siemens Networks commissioned a study on consumer privacy amongst mobile users:
 - 9,200 interviews worldwide
 - 14 countries
 - 16 – 65 year old mobile users



Source: NSN Consumer Privacy Study 2009

NSN Consumer Privacy Study Conclusions

- Globally **82%** believe privacy is an important topic
 - 76% have a high degree of concern about privacy violations
 - **People object strongly when their private information is used contrary to their expectations or without their permission**
- **53%** claim to be selective when sharing data
 - Differences in perception of sensitive information
 - Mismatch between attitudes and behaviour
 - many people shared sensitive information in online communities
 - Many willing to trade privacy for tangible rewards, provided partners are credible and sensitive material is handled properly
 - **Trust is key to reducing privacy concerns**
- **69%** would welcome a single portal to manage their personal information
 - A trusted server

Smartphones are no longer “phones”

- Global mobile data grew 2.6x in 2010 to 237 petabytes/month
 - 3x the entire data traffic on the global internet in 2000
 - Mobile video now 50% of all mobile data
- Mobile search set to overtake fixed search within 2 years



App's are now driving User Experience

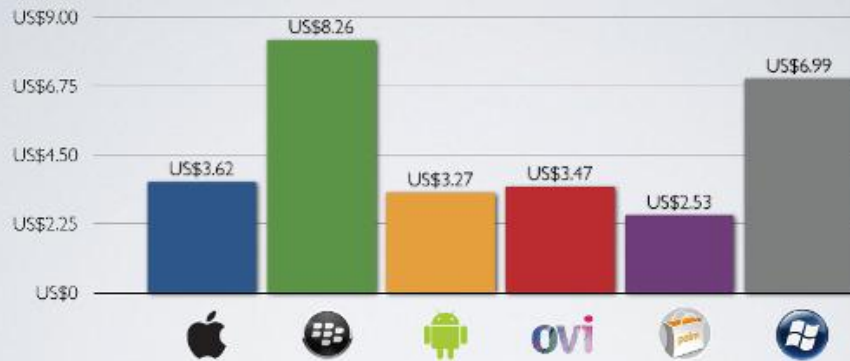


- Apple achieves 10 billion downloads

Distimo – US market, 2010

PRICE COMPARISON

Average price for all paid apps

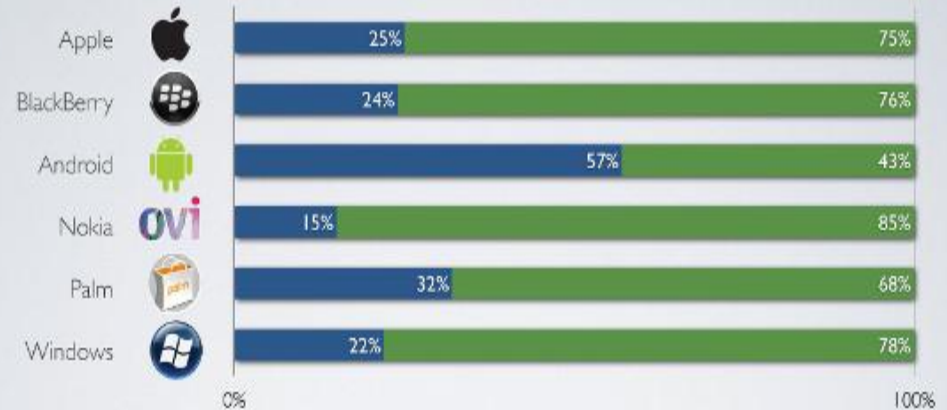


Distimo – US market, 2010



FREE VS PAID

■ Percentage Free ■ Percentage Paid



WSJ

Wall Street Journal's -
 "What they know" series

- Review of data privacy for popular App's

App name	Username, Password	Contacts	Age, Gender	Location	Phone ID	Phone number
Angry Birds	Blue	Light Blue		Purple	Red	
Angry Birds Lite	Blue			Purple	Red	
Aurora Feint II: Lite	Blue				Red	
Barcode Scanner (BahnTech)					Red	
Bejeweled 2	Blue					Pink
Best Alarm Clock Free				Purple	Red	
Bible App (LifeChurch.tv)				Purple	Red	
CBS News				Purple	Red	
Dictionary.com				Purple	Red	
Doodle Jump	Blue				Red	
ESPN ScoreCenter	Blue			Purple	Red	
Facebook	Blue	Light Blue		Purple		
Fluent News Reader				Purple	Red	
Foursquare	Blue		Blue	Purple		Pink
Fox News				Purple	Red	
Google Maps	Blue			Purple		
Grindr			Blue	Purple	Red	
Groupon	Blue			Purple	Red	
Medscape	Blue			Purple	Red	
MyFitnessPal			Blue	Purple	Red	
Netflix	Blue			Purple	Red	
NYTimes				Purple	Red	
Ninjump				Purple	Red	
Pandora			Blue	Purple	Red	
Paper Toss				Purple	Red	
Pimple Popper Lite				Purple	Red	
Pumpkin Maker				Purple	Red	
Ringtone Maker Pro	Blue				Red	
Shazam				Purple	Red	
Talking Tom Cat	Blue			Purple	Red	
TextPlus 4	Blue	Light Blue	Blue	Purple	Red	Pink
The Moron Test				Purple	Red	
TweetDeck	Blue			Purple		
The Weather Channel				Purple	Red	
WhatsApp Messenger						Pink
Yelp	Blue			Purple	Red	
YouTube	Blue					

Why is location important?

- Internet advertising market worth >\$50 bn today
- Typical internet advertising Cost Per Mille (CPM) ~\$3 (excluding SNS)
 - SNS average CPM ~\$0.6
- Typical Click Through Rate (CTR) for banner ad <0.1%
 - SNS CTR ~0.05%
- One (JiWire) market research study in Feb 2011 showed:
 - CTR 34%
 - 20% actually visited nearby shop location, 17% purchased in shop
- Location based advertisements currently command a 6 ~ 10 x premium on CPM

Consumers are becoming increasingly concerned about their data online:

73-86%
of Americans
say they do not want
tailored advertising
when told about common
ways data is gathered

Ref: Americans Reject Tailored Advertising by Joseph Turow and others



What can location reveal?

- Song et al., *Science* 327, 1018 (2010) analysed the anonymised data of 50,000 mobile users and were able to predict mobility with a probability of 93%
 - Indicating that user locations can be predicted
- Eagle & Pentland, *Personal & Ubiquitous Computing*, Vol 10, 255-268 (2006) demonstrated the ability to associate location with user behaviours
 - They identified business school students
 - Nathan Eagle and Alex Pentland. (2009) “Eigenbehaviors: Identifying Structure in Routine”, *Behavioral Ecology and Sociobiology*, 63:7, 1057-1066.
- And then there is
 - Scans Twitter for check-in locations that are being tweeted



PLEASE ROB ME

Protecting privacy

- Challenges for protecting privacy on mobile internet include:
 - Protect users' whereabouts
 - Protect users' community membership
 - Facilitate effective group communication without revealing sensitive information
 - Measure and visualise privacy
- The following slides present 3 alternative approaches to privacy protection:
 - Privacy-triggered networking – “hiding in a crowd”
 - Privacy Broker – autonomous authentication
 - Mobile Millennium – privacy enabled location based services



Privacy-triggered networking

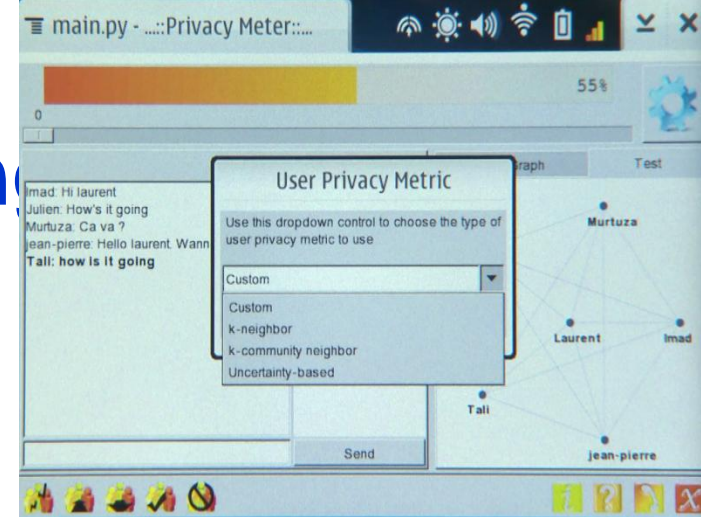
Privacy-Triggered Social Networking

- Allows consumers to communicate locally without revealing their identity
“Hiding in a crowd”
- Demonstrated using Wi-Fi for localised micro-blogging
 - Bluetooth/Wi-Fi allow peer-to-peer ad hoc mesh networks to be generated
 - Spontaneous network creation
 - Zones of metres to hundreds of metres
- Technology provides means to:
 - Visualize privacy level
 - Control communications by privacy settings



Privacy-Triggered Networking

- Mobile receiver continuously monitors radio signals
 - Identifies number of users present
- User defines level of acceptable anonymity
 - i.e. how many people there must be in the local “crowd”
 - K-space
- When user wishes to send a privacy enhanced message they:
 - Write message and press send
 - Application monitors radio signals and waits until the threshold minimum privacy level is attained
 - Only when threshold is achieved, message is sent
- Allows localised spontaneous networking without release of precise location
 - Area bounded by available nodes in ad hoc network

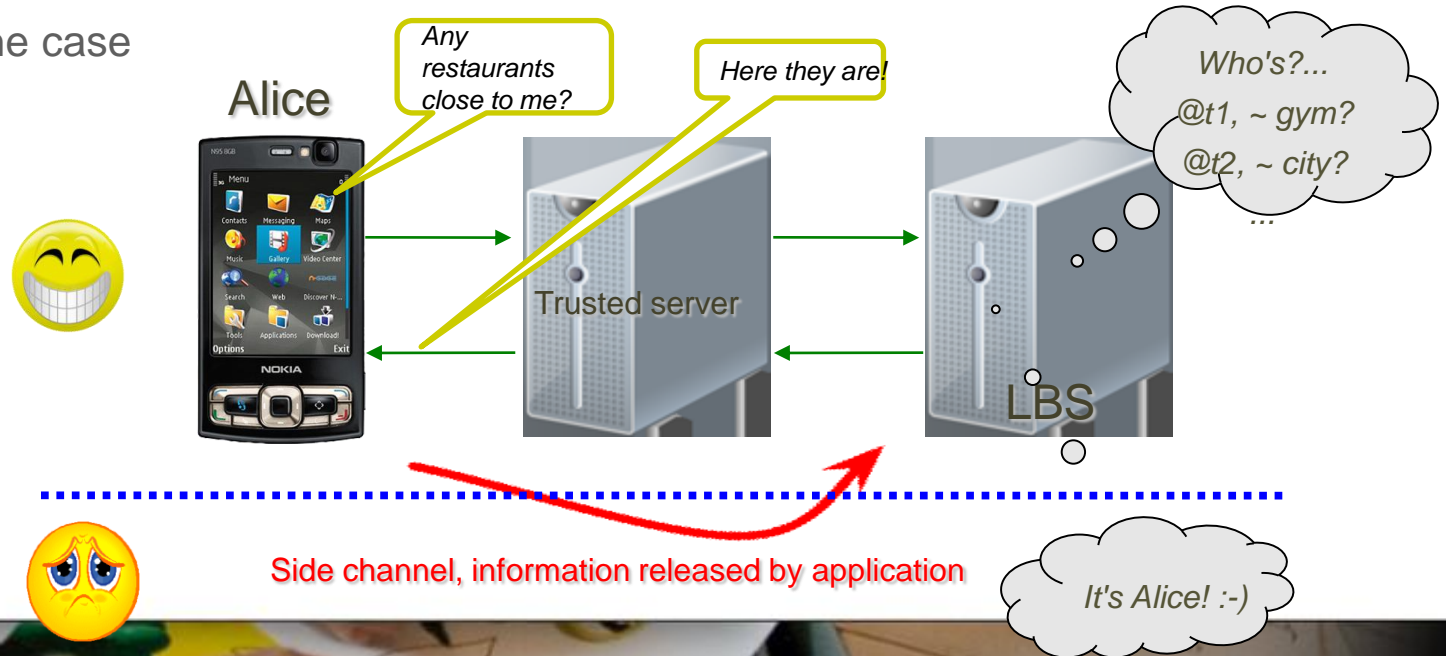




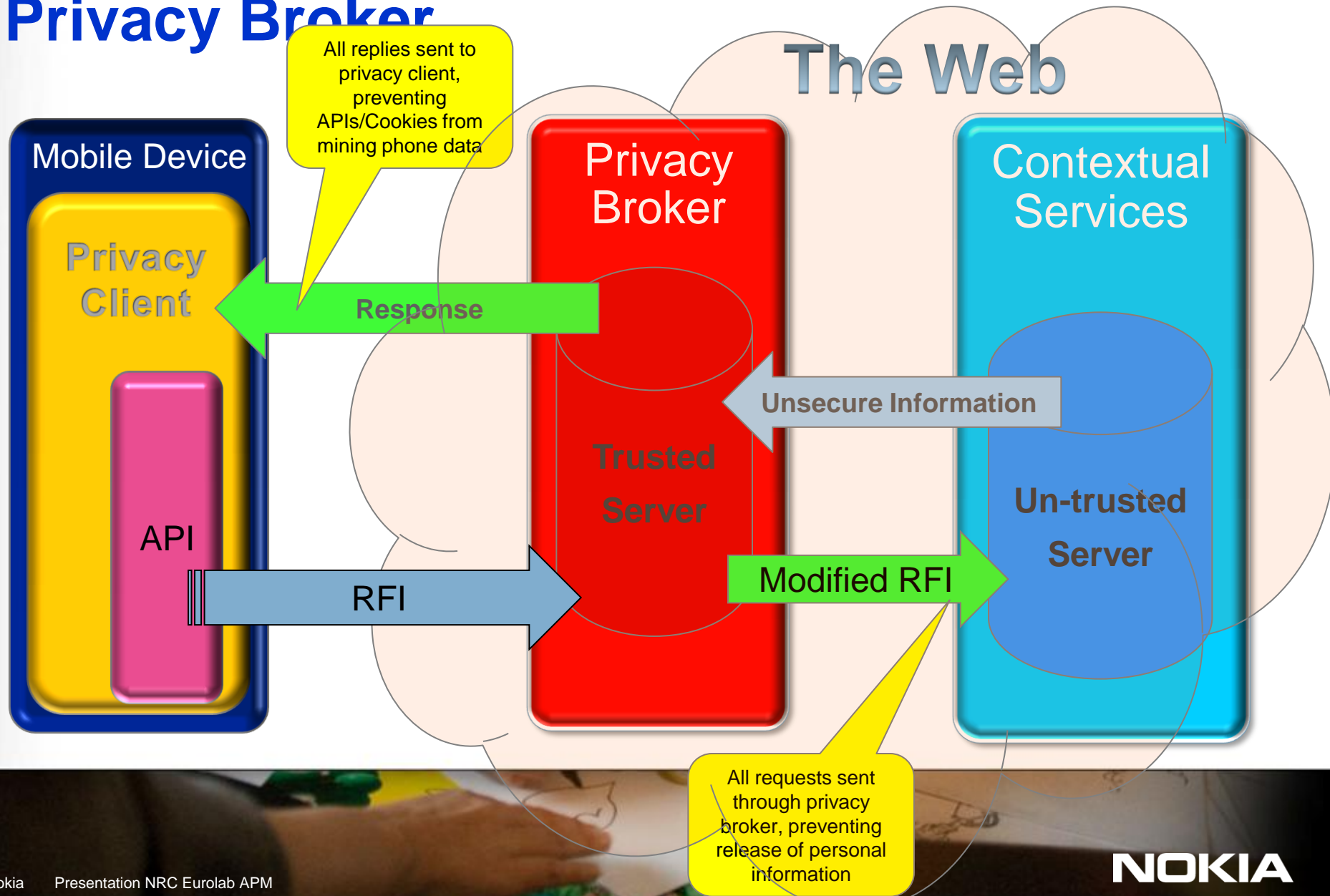
Privacy Broker

Privacy-Broker: legacy solutions

- Typical approaches involve a “trusted server”, acting as a “proxy” between users and third party services
 - The trusted server anonymises and/or blurs all information sent by the user as it leaves the proxy server
- However, these approaches assume that the client application is “trusted”
 - Often not the case



Privacy Broker



Privacy Broker – achievements to date

- Two location based services have been demonstrated using the privacy broker:
 - LBS Pull service
 - A city visitor finds points of interest using predefined preferences (such as favourite shops, art or work interests, etc.)
 - Preferences either entered or learned from contextual mining
 - LBS Push advertising service
 - Promotions in locality based on pre-defined user preferences
- Privacy is maximised for each application by:
 - Determining minimum required data for service
 - Minimising transmission of data (aggregating at source)
 - Minimising stored data (aggregating at Privacy Broker)



Mobile Millennium

Mobile Millennium

- Aims to provide real-time travel information to consumers with no infrastructural requirements
 - (other than existing telecommunications equipment)
 - Consumer GPS data set to dwarf other traffic data sources

- Public-Private-Academic partnership



- Full end-to-end system developed using large scale pilots and field tests

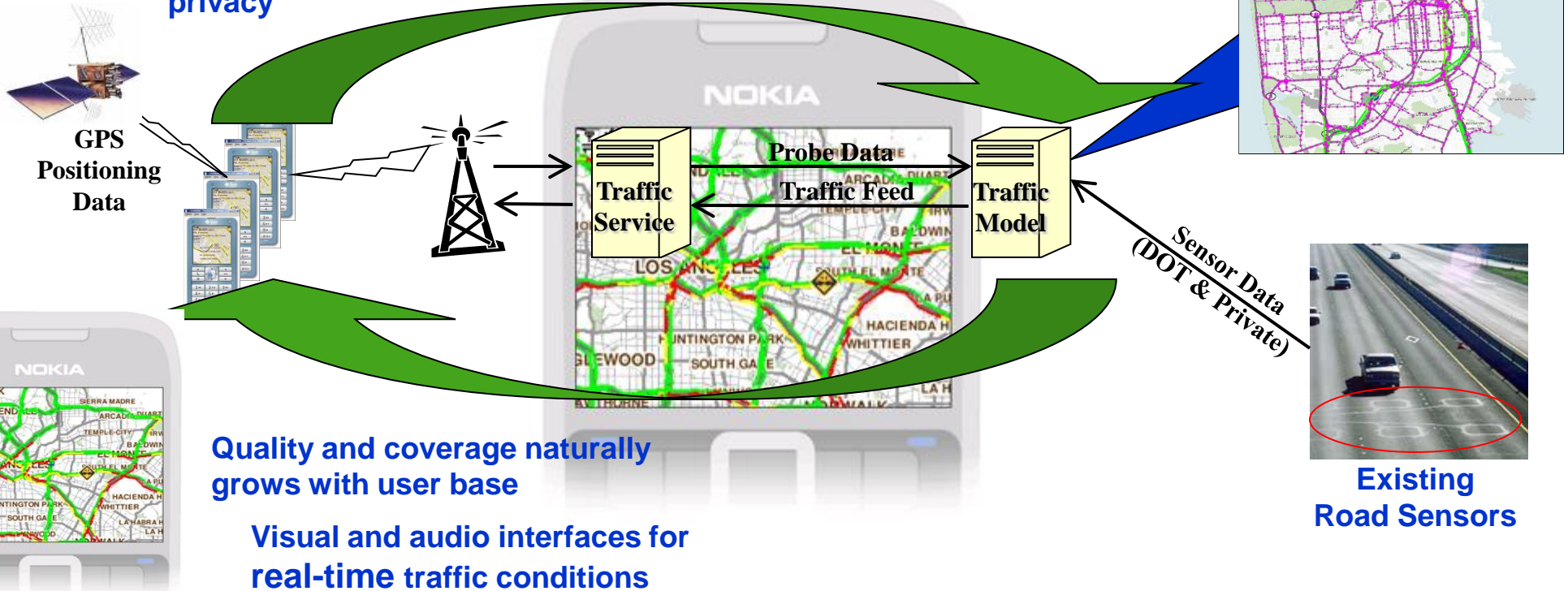


Mobile Millennium

Crowd Sourcing Automotive Traffic Conditions

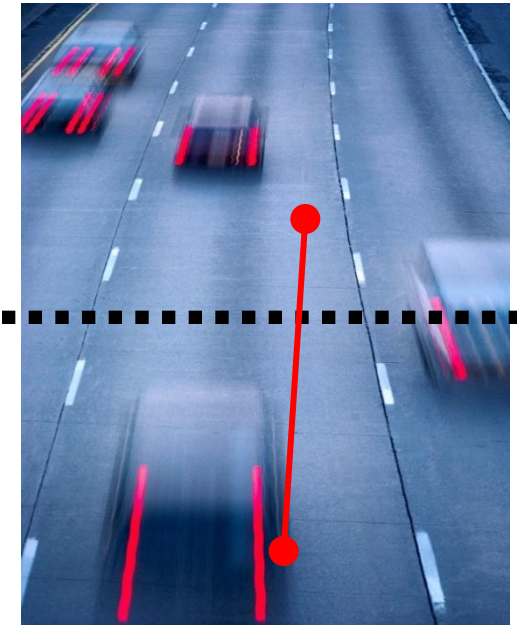
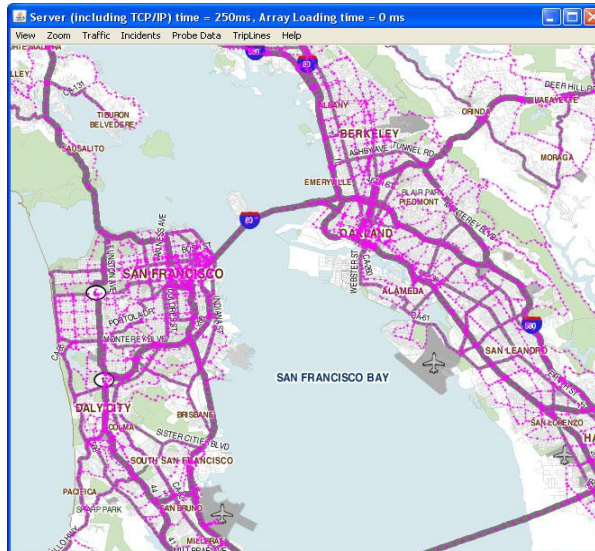
Users contribute GPS measurements of local traffic conditions
Data collection optimized for efficiency & privacy

Data aggregated with other sources for processing

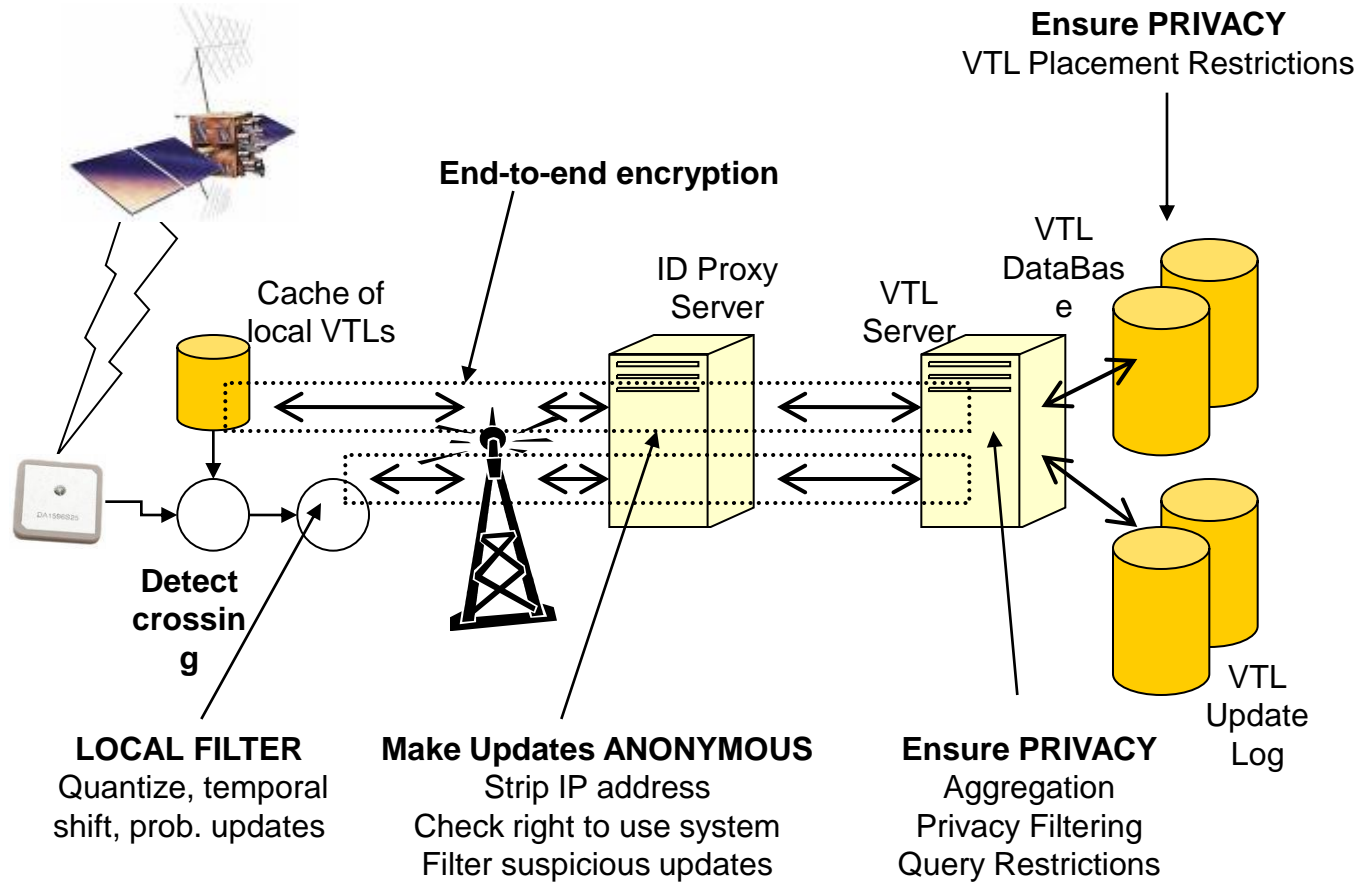


Virtual Trip Lines for Data Collection

- Virtual lines at intelligently placed locations
 - Server requests client to report at given Virtual Trip Line locations
 - Trip line placement calculated to maximise traffic analysis accuracy and **privacy**
 - Mobile uses GPS to detect crossing of trip lines
 - Anonymously reports crossing with speed & travel time
 - Data is distorted and temporally shifted



Mobile Millennium



Privacy in contextual services

- Alignment of technical solution with the 7 principles of Privacy by Design:

Source: Dr Ann Cavoukian, Information & Privacy Commissioner, Canada

- **Proactive and preventative** – minimum information collected, transmitted and stored. Sensitive information discarded as early as possible
- **Providing privacy by default** – opt in required to use service, speed reported as percentage of local limit with maximum of 100%
- **Privacy embedded in the design** – system inherently privacy protecting
- **Positive-sum full functionality** – provides users with enhanced traffic services and maintains privacy
- **End-to-end lifecycle protection** – yes, users' IP address and location not stored
- **Visibility and transparency** – consumer is in control with visibility of privacy settings, data usage and ability to opt out at any time
- **Respect for user privacy** – Consumer is nucleus for innovation

Privacy Target State

*Consumers Trust
Nokia To Fulfill
Their Privacy
Expectations*

NOKIA