Game-Theoretic Model of Incentivizing Privacy-Aware Users to Consent to Location Tracking

Emmanouil (Manos) Panaousis, Aron Laszka, Johannes Pohl, Andreas Noack, and Tansu Alpcan

Secure and Dependable Software Systems (SenSe) Research Group
School of Computing, Engineering and Mathematics

University of Brighton

Some Info…

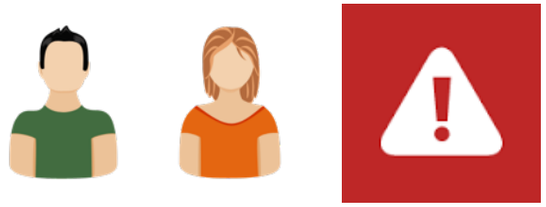
- Brighton is a seaside resort and the largest part of the city of Brighton and Hove situated on the south coast of England

- I am a lecturer with the University of Brighton, which is a UK university of over 21,000 students and 2,500 staff based on five campuses in Brighton, Eastbourne and Hastings on the south coast of England

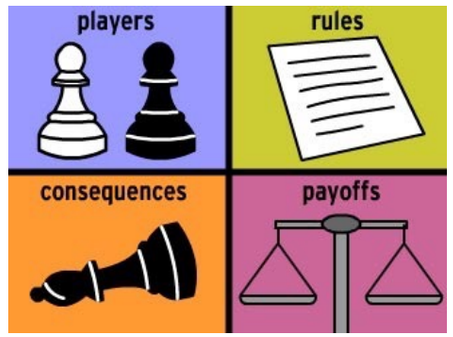
- There I am art of the SENSE (Secure and Dependable Software Systems) research group led by Prof Mouratidis

Motivation

- Prevalence of smartphones brings to end users not only new applications and services but also privacy risks



- Location privacy is one of these...

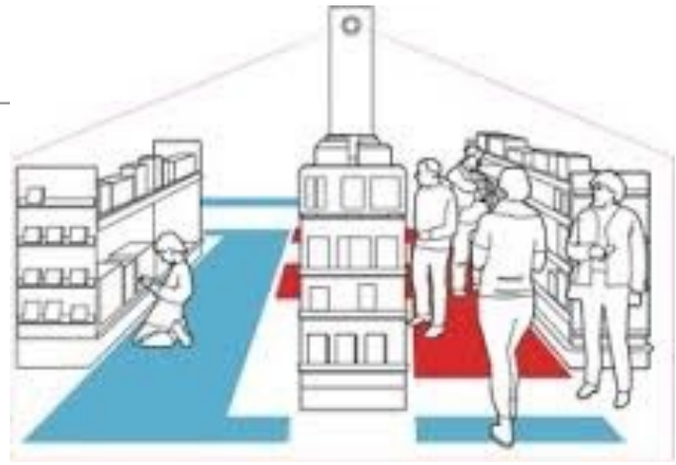


- We propose a game-theoretic model to capture the interaction between a Company and a User

- The Company offers some services to the User, while he is connected to a WLAN that belongs to the Company

- We investigate how location privacy is affected by the amount of time a User is connected to a wireless local area network (WLAN)

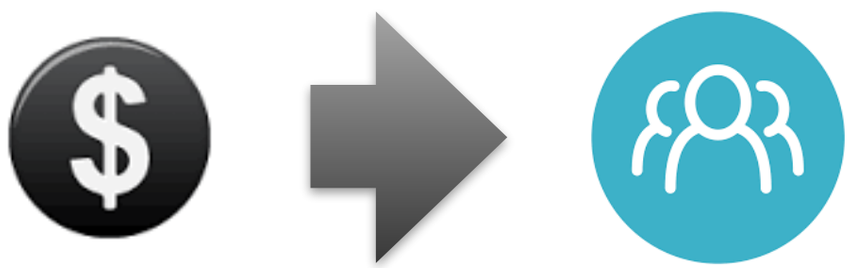
How Users' Data Can Be Used



- **Optimization of stores**: the Company can optimize the store design based on heat-maps of customer movements

- **Targeted advertisements**: if the Company knows the location of customers, it can send product information based on their location, creating location-based spam

- **Profiling**: from the User's long-term location information, the Company can create profiles, and use them for strategic decisions, or even sell this information to third parties



Localization Attack Examples

- In 2013, a UK startup sniffing out passing Wi-Fi signals from mobile phones, and snaffling location data without users' consent

http://www.cnet.com/news/londons-smart-bins-track-4m-phones-a-week-over-wi-fi/

- In 2015, researchers (Stanford University) designed an Android app to measure changes in battery use which over time allowed them to locate phones with up to 90 percent accuracy.

http://www.techtimes.com/articles/34812/20150223/gps-android-stanford-rafael-powerspy.htm

User Localization

highest possible additive level of the offered services

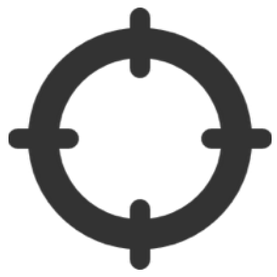
User

$l(\tau)$

User mobile phone connected to WLAN

t: connection time
T: roaming time
δ: is the minimum connection time

Company



Localization System

$l_{est}(\tau)$

Estimated user location

$0 < S \leq S^*$

service level

The localization occurs without the User's active participation

Model Parameters

$p(t) := \frac{T}{t}\hat{l}$ User's **location privacy** when connected for t

Any position estimate is biased with an error

$l_{err}(\tau) := \|\boldsymbol{l}(\tau) - \boldsymbol{l}_{est}(\tau)\|$

$\hat{l} := \mathbb{E}[l_{err}(\tau)]$

$$\sigma(t, S) := \frac{t}{T}S$$

when t increases $\Rightarrow$ $\boldsymbol{l}_{est}(\tau) \rightarrow \boldsymbol{l}(\tau)$ $\Rightarrow$ 

received service level


location privacy

S

provided service level


User decides t

- t: too high → too low location privacy
- t: too low → too low experienced service level

Multiple Users

There are multiple User types; User of type $i \in \mathcal{A}$

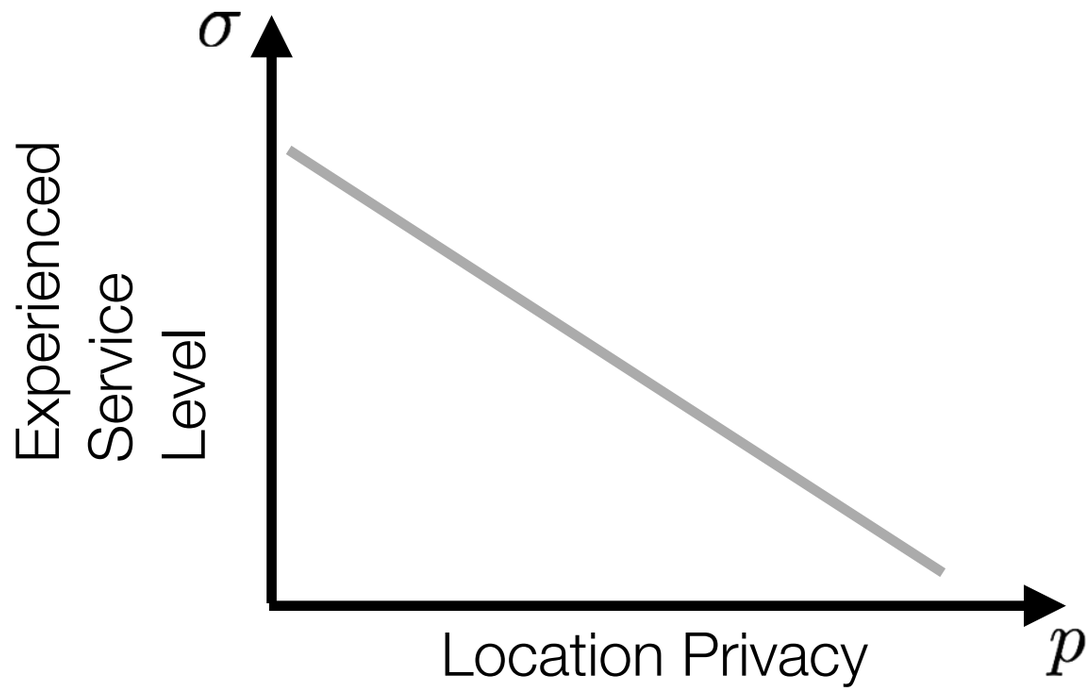
a_i : probability of User to be of type i

Π_i

preference to protect location privacy

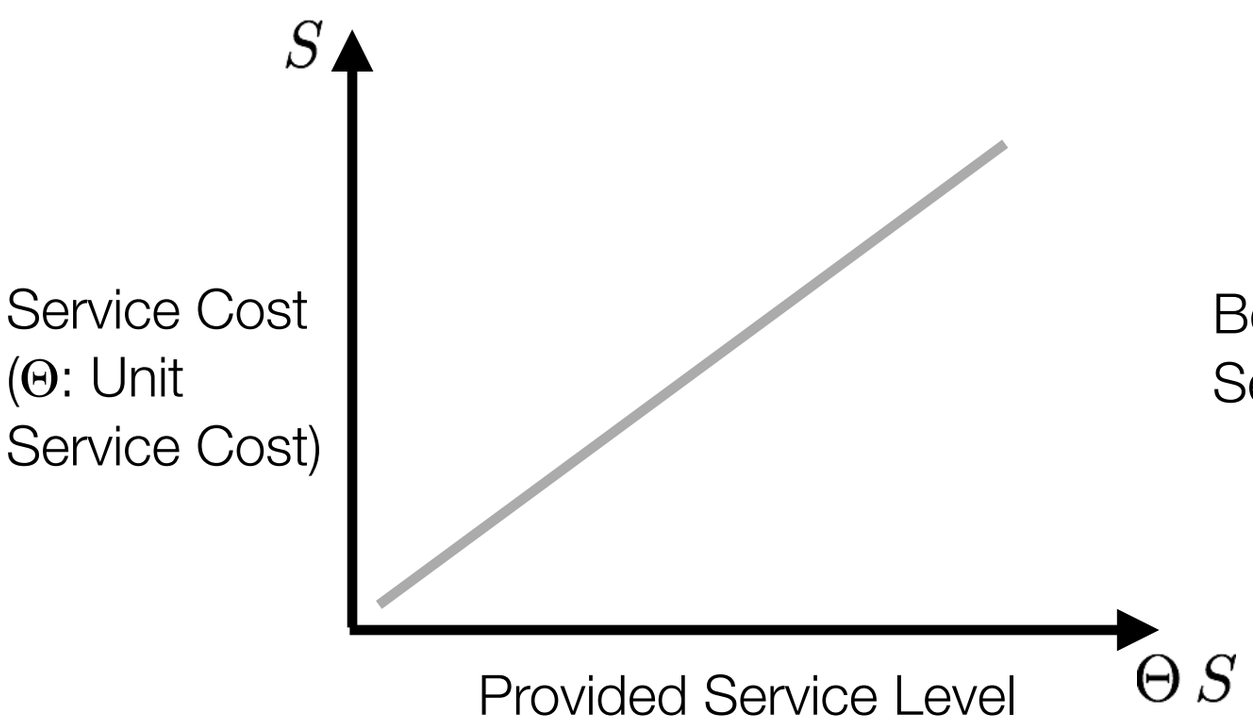
$\Pi_i = 1$ → User who completely ignores the service provided by the Company in favor of maximizing his privacy

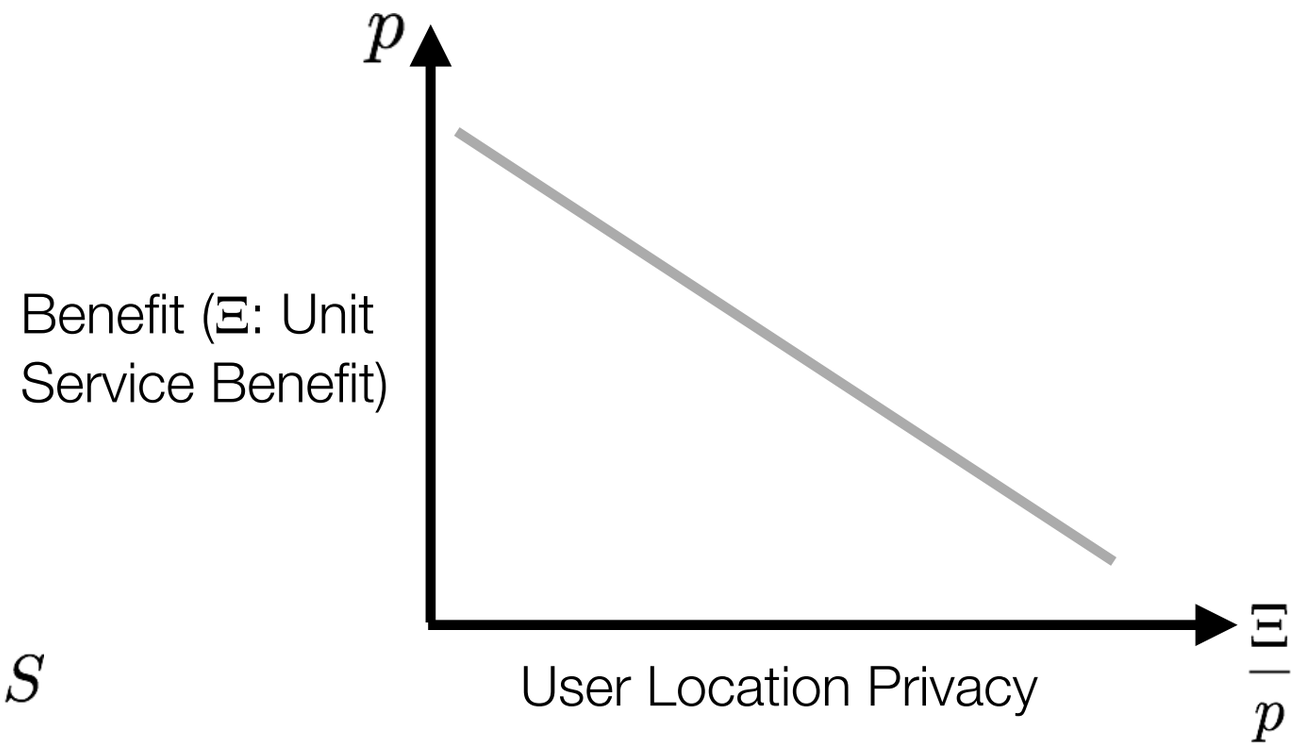
$\Pi_i = 0$ → User who is not concerned about his location privacy at all



optimal t maximizes Π_i **x location privacy +** $(1 - \Pi_i)$ **x experienced service level**

Company





- S: too high → too high service cost but it can motivate User to get connected for longer and therefore User Location Privacy decreases → high benefit
- **optimal** value of S maximizes **benefit - service cost**

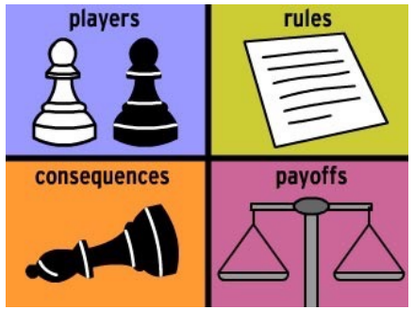
1) optimal t should consider Company's advertised service level
2) optimal S should take Users' different types and strategies into account

Strategic interaction between players

Game Theory

Game-Theoretic Model

User



Company

- Each User type selects t_i
- User's pure strategies $\mathcal{S}_U := [\delta, T]$
- A player's mixed strategy is a distribution over the set of his pure strategies
- The User plays **only pure strategies**, since there always exists a pure strategy that is a **best response** to the advertised service level

- Company's pure strategies $\mathcal{S}_C := \{1, \ldots, S^*\}$

  $\mathbf{\Phi}$: mixed strategy of the Company an $|\mathcal{S}_C|$-dimensional vector

  ϕ_j : probability of offering *j*-th service level

- Company advertises an expected service level $\hat{S} := \sum_{j \in \mathcal{S}_C} \phi_j \, S_j$
- Therefore for any $\hat{S} \in [\min_{j \in \mathcal{S}_C} S_j, \max_{j \in \mathcal{S}_C} S_j]$ there is a one-to-one mapping $\mathbf{\Phi} \Leftrightarrow \hat{S}$

Game-Theoretic Model (contd.)

Location Privacy Game (LPG): Stackelberg (leader-follower) game: the **leader** (**Company**) first commits to his strategy, which is observed by the **follower** (**User**)

User

- For a given strategy profile $(\hat{S}, t_i)$

$$\begin{aligned}\mathcal{U}_U^{(i)}(\hat{S}, t_i) &:= \Pi_i\, p_i + (1-\Pi)\,\sigma(t_i, \hat{S}) \\ &= \frac{\Pi\, T\, \hat{l}}{t_i} + (1-\Pi_i)\,\frac{\hat{S}}{T}\,t_i \\ &= \Psi_1\,\frac{1}{t_i} + \Psi_2\,\hat{S}\,t_i\end{aligned}$$

location privacy

experienced service level

Company

- For a given User *i* and $(\hat{S}, t_i)$

$$\begin{aligned}\mathcal{U}_C^{(i)}(\hat{S}, t_i) :&= \frac{\Xi}{p_i} - \Theta\,\hat{S} = \frac{\Xi}{T\,\hat{l}}\,t_i - \Theta\,\hat{S} \\ &= \Psi\, t_i - \Theta\,\hat{S}\end{aligned}$$

- Company's overall expected payoff

$$\begin{aligned}\mathcal{U}_C(\hat{S}, \boldsymbol{t}) &= \sum_{i\in\mathcal{A}} \alpha_i \cdot \mathcal{U}_C^{(i)}(\hat{S}, t_i) \\ &= \sum_{i\in\mathcal{A}} \alpha_i \cdot (\Psi\, t_i - \Theta\,\hat{S})\end{aligned}$$

benefit

service cost

User's Optimal Strategy

Lemma 1: For any Company strategy $\hat{S}$ the User's best response is either δ or T

Theorem 1: If User of type i plays a best-response strategy and breaks ties in favor of the Company, then his strategic choice for a Company strategy $\hat{S}$ is

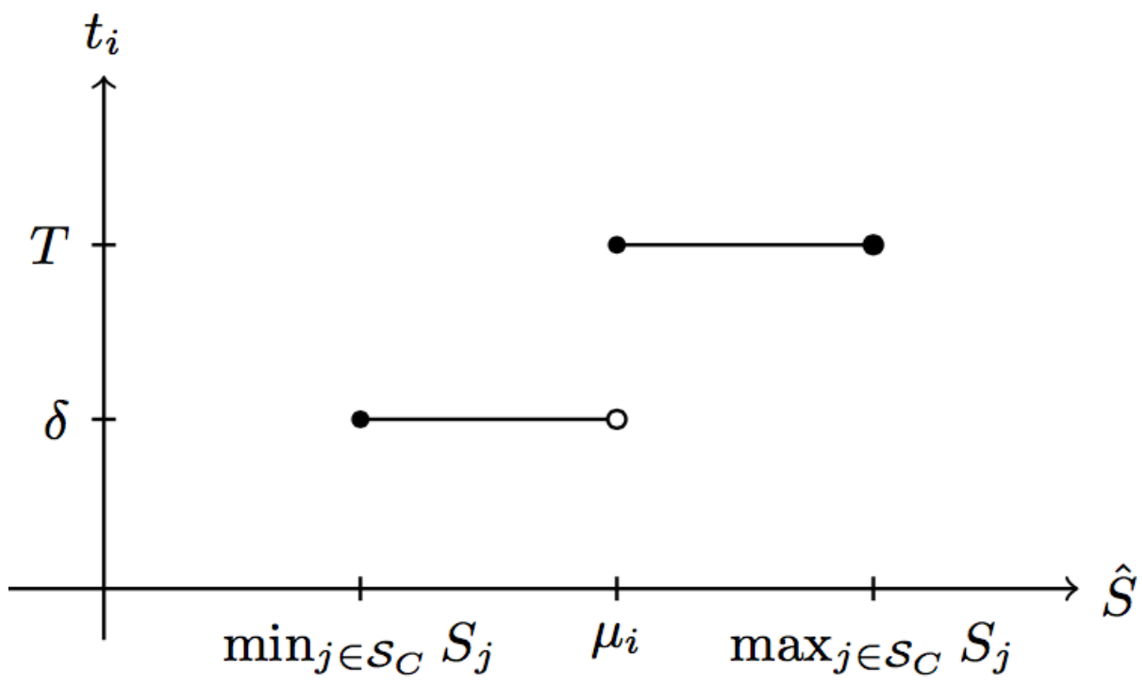
- $t_i = \delta$ if $\hat{S} < \mu_i$,
- $t_i = T$ if $\hat{S} \geq \mu_i$,

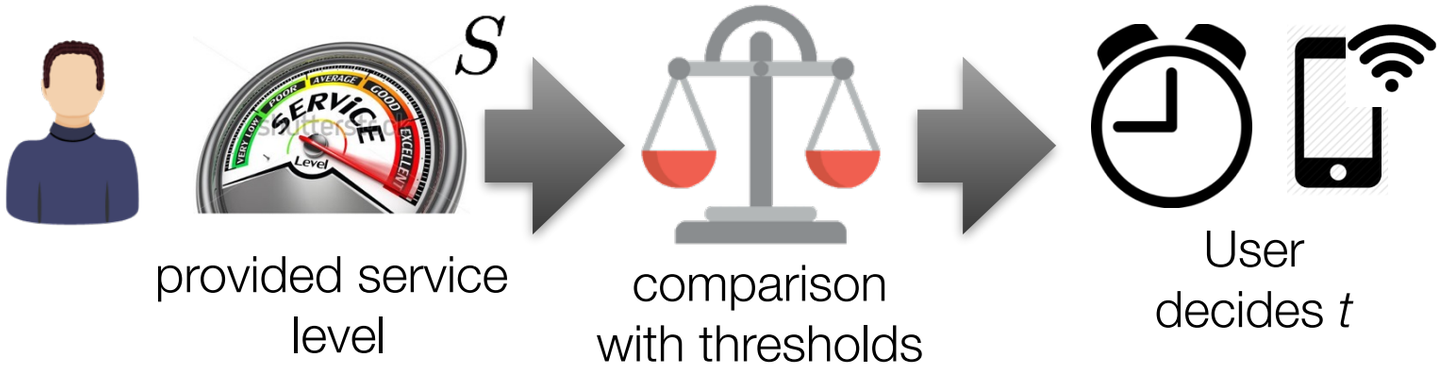
where

$$\mu_i = \frac{\Psi_1}{\Psi_2} \frac{1}{\delta T}.$$

$$\Psi_1 = \Pi_i \, T \, \hat{l}$$

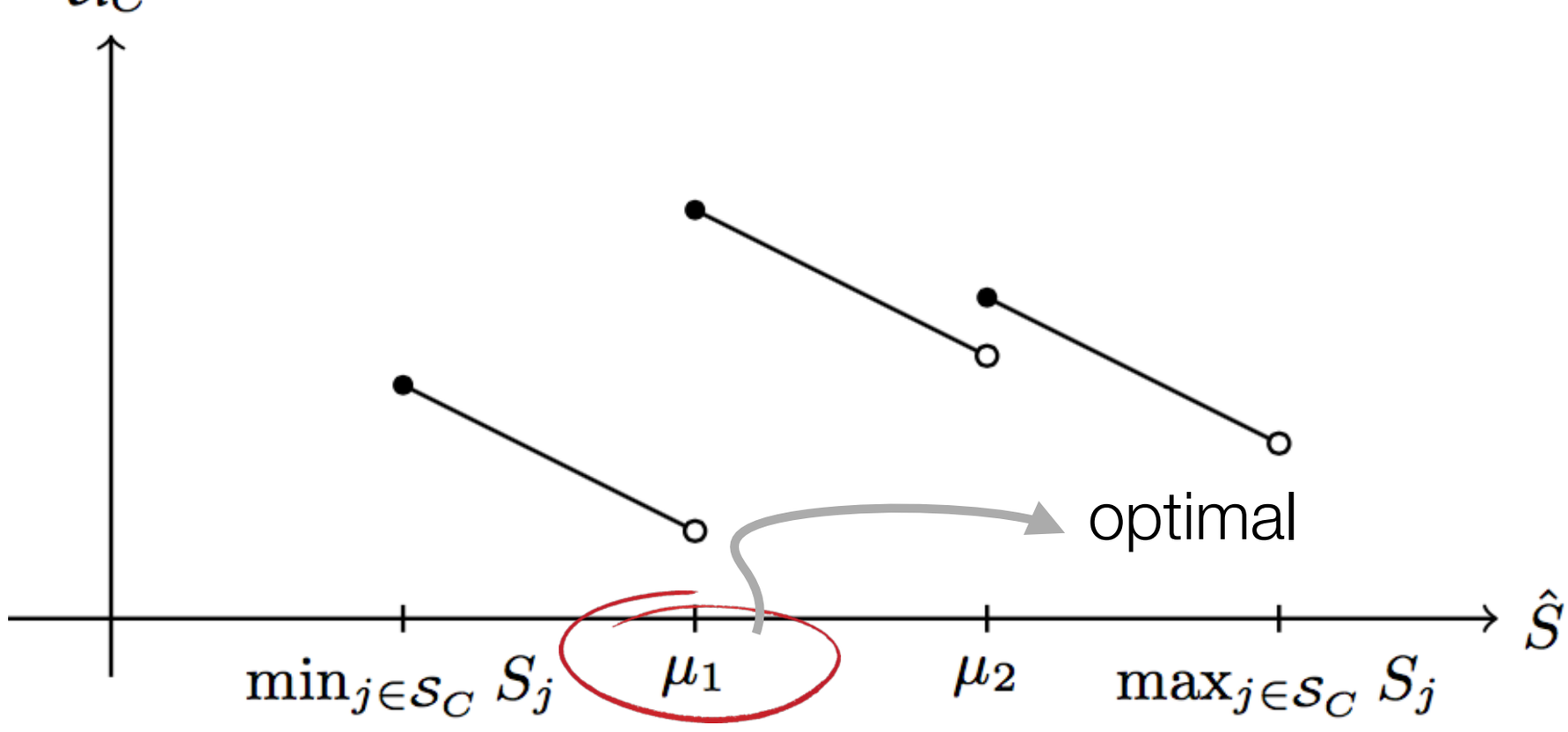
$$\Psi_2 = \frac{1 - \Pi_i}{T}$$





Company's Optimal Strategy

Theorem 2: The Company's optimal strategy is either $\min_{j \in \mathcal{S}_C} S_j$ or one of the threshold values μ_i defined in Theorem 1.

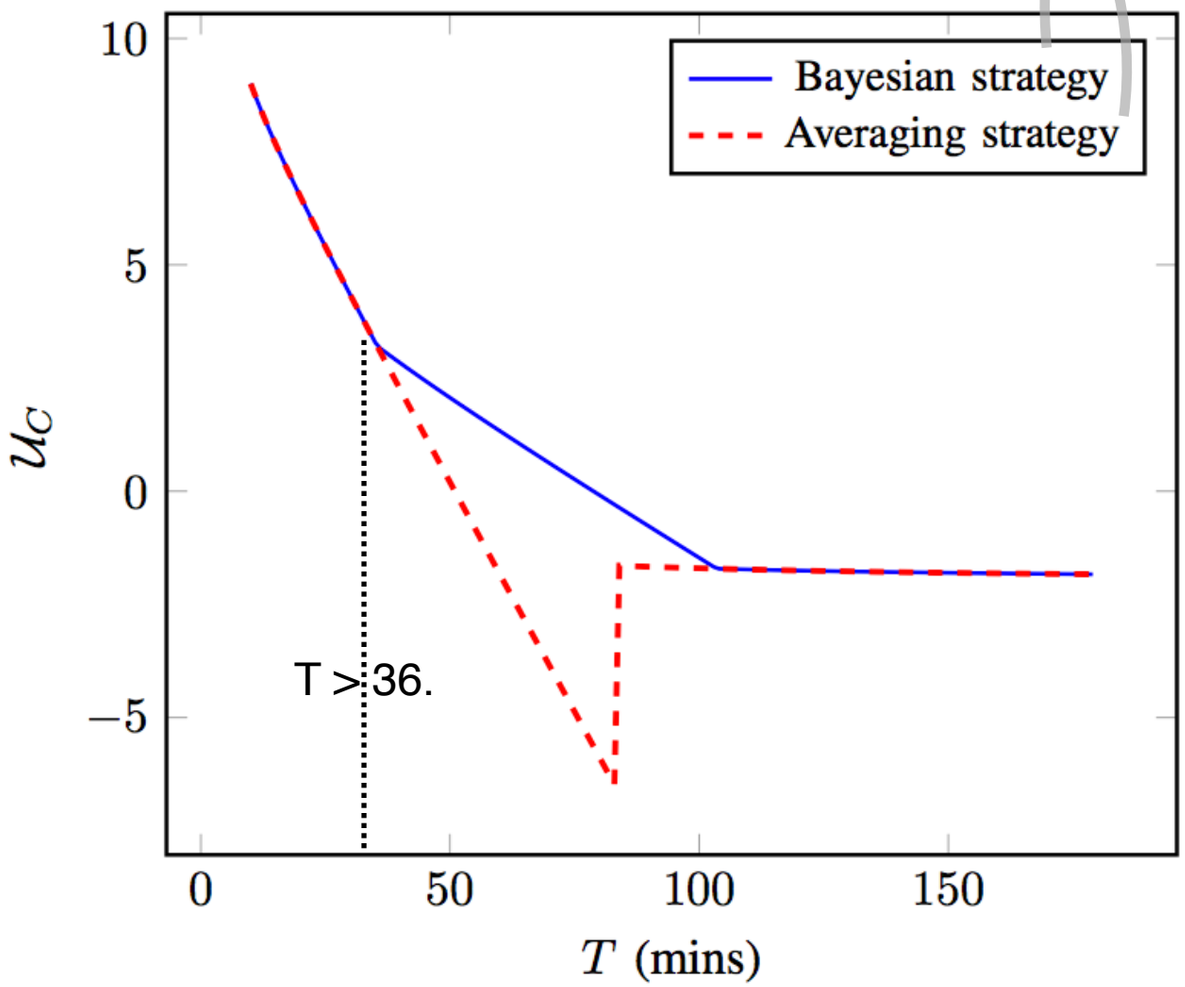


Numerical Examples

- unit service benefit Ξ is 50% higher than the unit service cost Θ
- localization error equals 2 meters
- users' classification
  - **Privacy Fundamentalists (PF)**: reject the consumer-benefit or societal-protection claims for data uses and seek legal- regulatory privacy measure
  - **Privacy Unconcerned (PU)**: ready to supply their personal information to business and government and reject what is seen as too much privacy fuss
  - **Privacy Pragmatists (PP)**: examine the benefits of the data collection and use, want to know the privacy risks and how organizations propose to control those, and then decide whether to trust the organization or seek legal oversight
  - For demonstration purposes we set the Π_i values as {0.2, 0.5, 0.8} for PF, PU, and PPs.

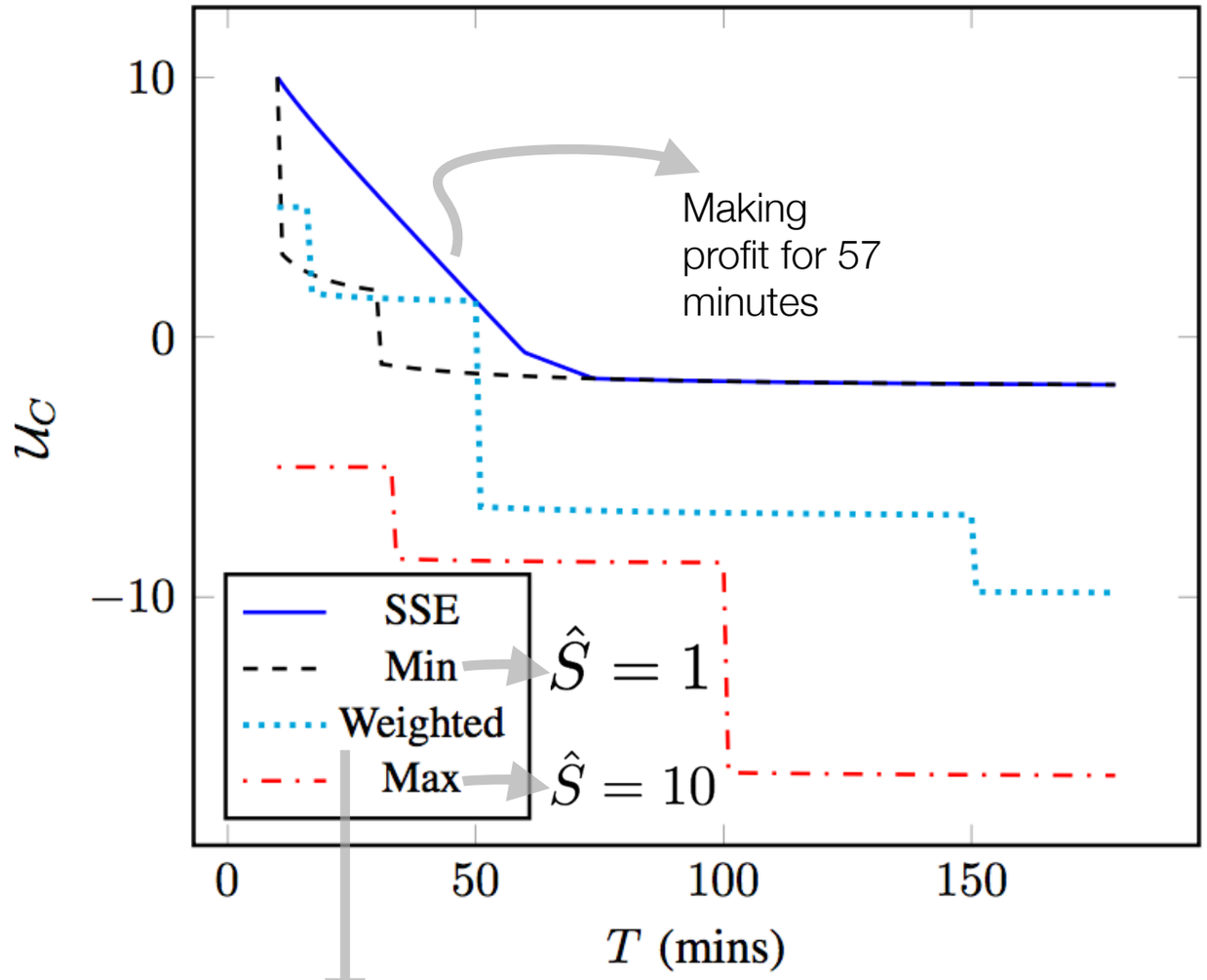
Numerical Examples - Results

$$\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \alpha_3] = [0.2, 0.55, 0.25]$$



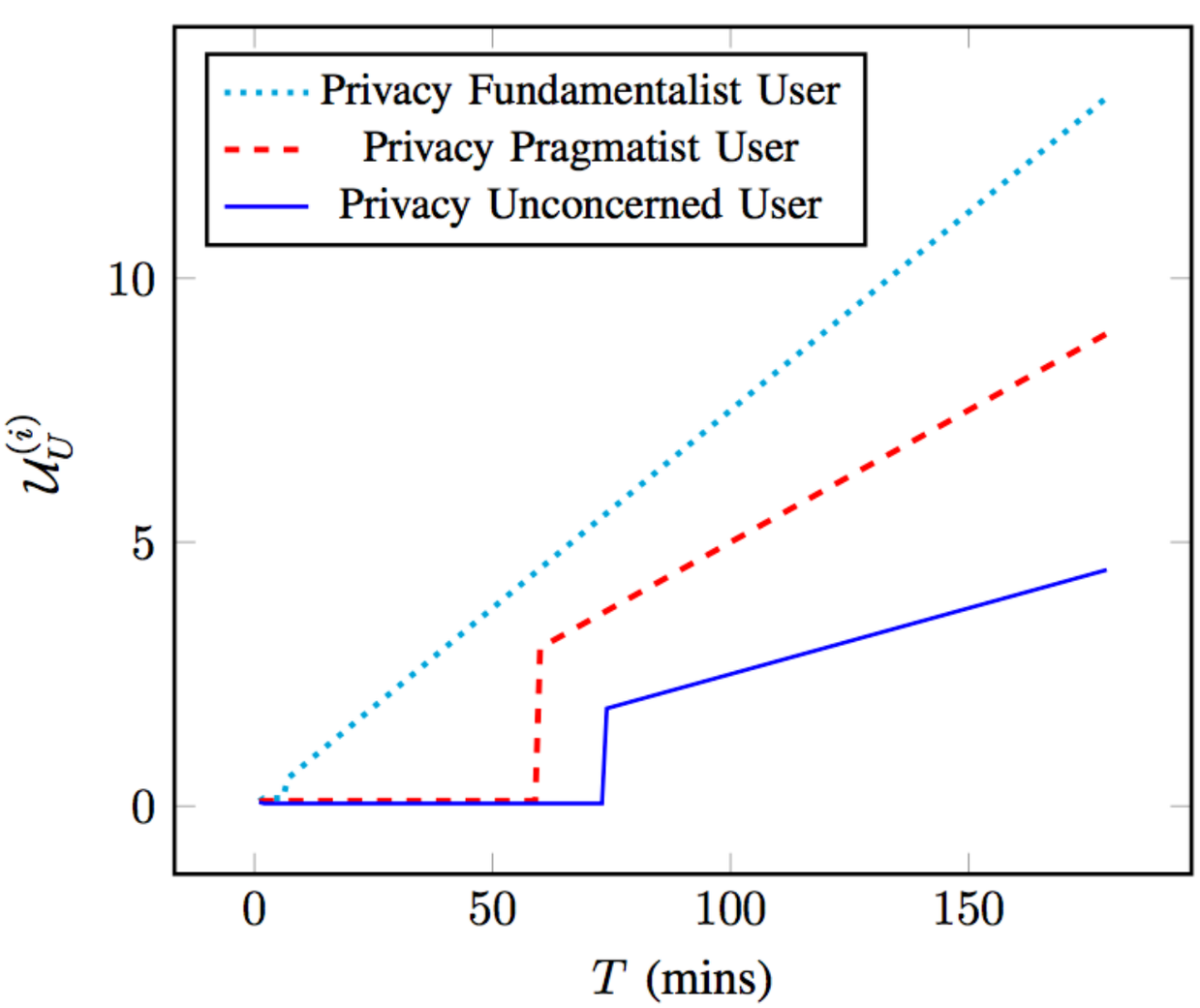
- Due to negative payoffs after some points in time, the Bayesian strategy gives 31 minutes extra time for the Company to make profit

it considers a single User type with privacy factor average value equal to 0.5

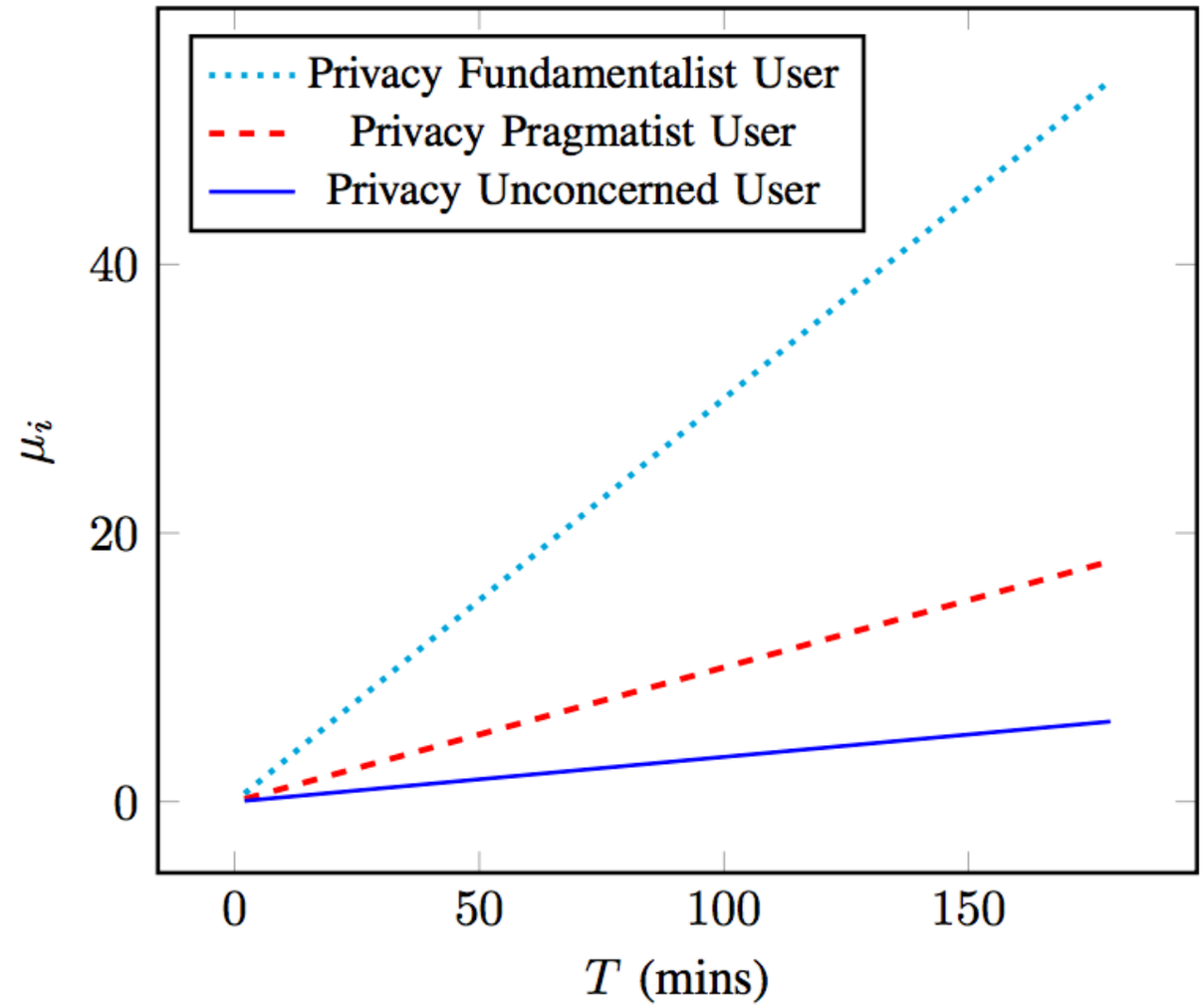


$$\hat{S} = 0.2 \cdot 2 + 0.55 \cdot 5$$
$$+0.25 \cdot 8 = \lfloor 5.15 \rfloor = 5$$

Numerical Examples - Results (contd.)



Payoffs of the different User types at the SSE of the LPG



- The higher T, the higher $\hat{S}$ must be for the User to stay connected for T
- For the same T, a PF User requires a 3 times higher $\hat{S}$ than a PP User, in order to stay connected for T, and 9 times higher $\hat{S}$ than a PU User

Conclusion & Future Work

- Conclusion
  - we proposed a game-theoretic model to analyze the trade-off between location privacy, the level of services that a user experiences, and the profit of the company.
  - we showed how to find optimal strategies efficiently
  - numerical results show considerable improvement
- Future work
  - modeling privacy loss as a nonlinear function
    - more likely to be logarithmic - initially any extra tracking information is useful for location prediction, but as we get more user data it does not improve the localization that much
  - incorporate user strategy for subscribed levels of service, which may be less than what is offered by the company
  - other privacy loss by users, including being profiled - what they like, demographics (this can be obtained if they subscribe to the offers), where they are located

Thank you for your attention!

Questions?