

INTRODUCTION À LA SÉCURITÉ INFORMATIQUE SÉANCE 3

Marc-Olivier Killijian

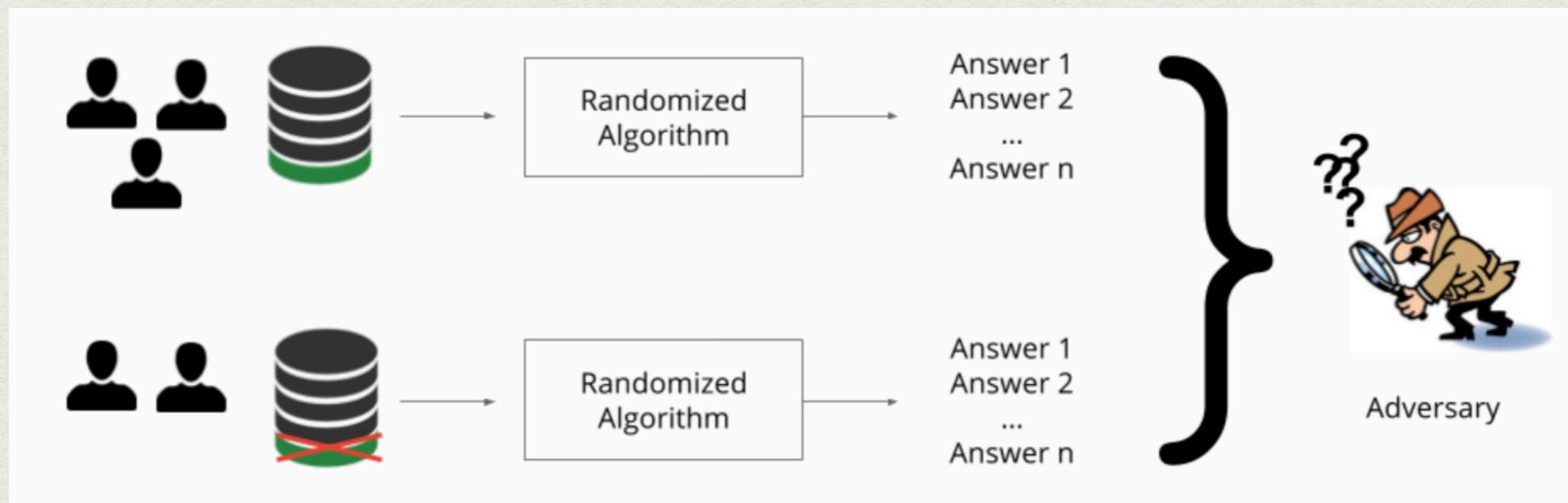
UQAM, CNRS

INF4471 A21

CONFIDENTIALITÉ DIFFÉRENTIELLE

CD? DP?

- Confidentialité Différentielle (CD) - *Differential Privacy (DP)* [Cynthia Dwork 2006]
- Déf. informelle: l'**absence ou la présence** d'un individu dans une base de données n'**influence pas le résultat** des requêtes à cette base sauf **faible probabilité**
 - Sinon le résultat permet d'inférer la présence ou l'absence de l'individu
- Fortes garanties de VP. **Robuste aux connaissances auxiliaires**



RÉPONSE RANDOMISÉE

- Techniques issue des sciences sociales pour collecter des statistiques sur des comportements embarrassants ou illégaux
 - Lancer une pièce
 - Si **pile**, répondre la **vérité**
 - Si **face**, lancer une autre pièce et répondre **OUI** pour **face** et **NON** pour **pile**
- **Utilité:** Permet la collecte de statistiques sur les participants ayant la propriété P (probabilité p) :
OUI : $3/4$ des individus qui ont P + $1/4$ des individus qui n'ont pas P
 $|OUI| = \frac{1}{4}(1 - p) + \frac{3}{4}p = \frac{1}{4} + \frac{p}{2}$
On peut donc estimer p : $p = 2|OUI| - \frac{1}{2}$
- **PVP:** La randomisation permet le **déni plausible** car une réponse OUI (ou NON) peut provenir d'un lancé de pièce

DÉFINITION ET BUDGET

Définition 2.1. (Differential Privacy) Un mécanisme randomisé \mathcal{A} satisfait la ϵ -differential privacy (ϵ -DP) si pour toutes bases de données D_1 et D_2 différant seulement d'un individu et pour n'importe quelle sortie $O \in Im(\mathcal{A})$, la propriété suivante est respectée :

$$Pr[\mathcal{A}(D_1) = O] \leq e^\epsilon \times Pr[\mathcal{A}(D_2) = O]$$

- ϵ : budget qui quantifie le niveau de protection du mécanisme
 - ϵ petit (proche de 0), garantie forte
 - ϵ grand, garantie faible (mais distorsion faible)
- **Comment fixer ϵ ?**

Documents de référence : [The Algorithmic Foundations of Differential Privacy - Dwork & Roth 2014](#)
[Differential Privacy: A Survey of Results - Dwork 2008](#)

SENSIBILITÉ D'UNE FONCTION

Définition 2.2. (Sensibilité Globale) Pour toutes fonctions $f : D \rightarrow \mathbb{R}^d$, sa sensibilité notée Δf est définie par :

$$\Delta f : \max_{D_1, D_2} \|f(D_1) - f(D_2)\|$$

pour tout D_1, D_2 deux bases de données différant par un seul individu.

- Δf : la sensibilité de la fonction f
 - paramètre très important qui mesure la contribution maximale d'un individu dans la base de données
 - En général, peut être difficile à calculer, voire à estimer mais cas simples comme les comptes:
 - $f = \text{nombre de chauves dans une BDD}$ $\Delta f = 1$
 - $f = \text{nombre de chauves arrondi à un multiple de } 5$ $\Delta f = 5$

MÉCANISME LAPLACIEN

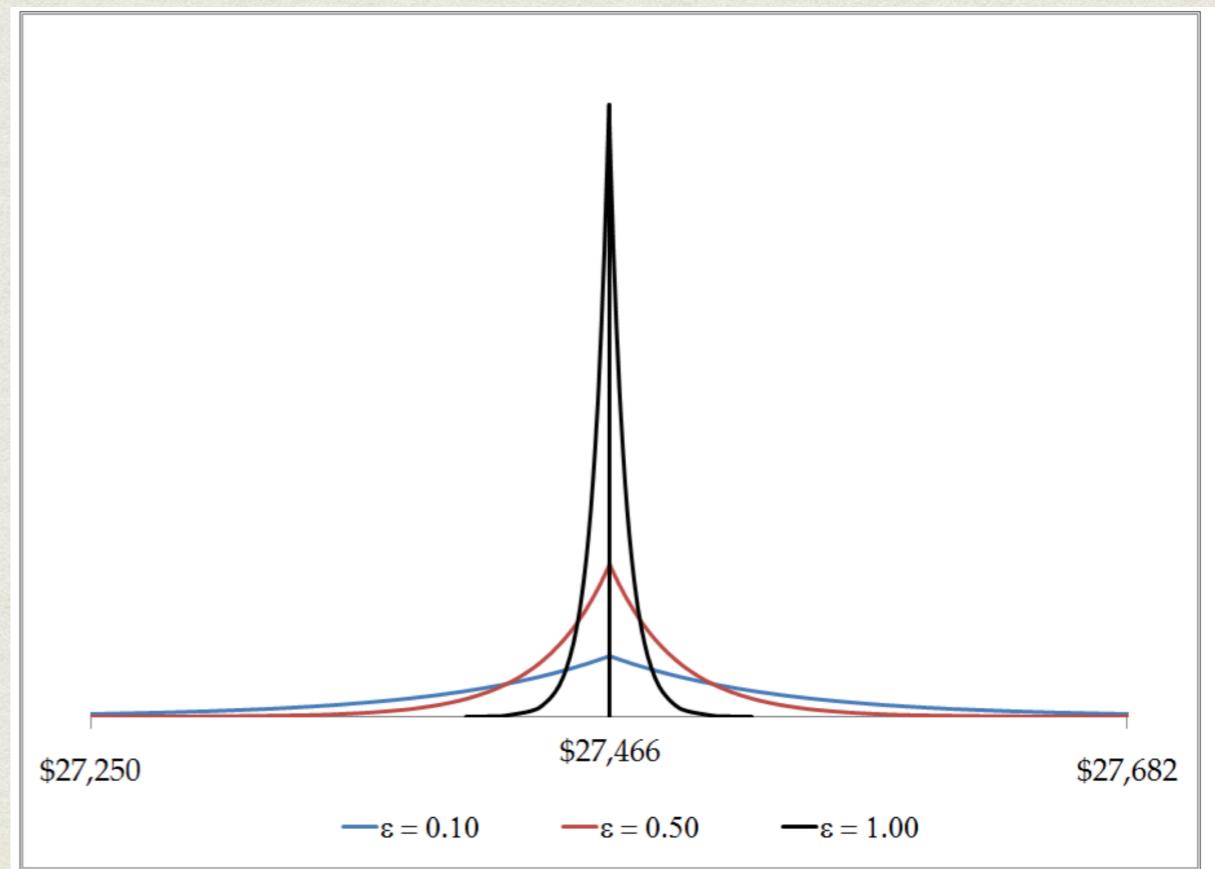
Définition 2.3. (Mécanisme Laplacien) Pour toutes fonctions $f : D \rightarrow \mathbb{R}^d$, le mécanisme \mathcal{A}

$$\mathcal{A}(D) = f(D) + (\mathcal{L}_1(\lambda), \dots, \mathcal{L}_k(\lambda))$$

est ϵ -DP si $\mathcal{L}_i(\lambda)$ sont des variables aléatoires indépendantes tirées de la distribution Laplacienne de paramètre $\lambda = \frac{\Delta f}{\epsilon}$

- Pour une fonction f avec k termes

- Si $k=1$: $\mathcal{A}(D) = f(D) + Lap\left(\frac{\Delta f}{\epsilon}\right)$
- $\epsilon \rightarrow 0 \Rightarrow Lap\left(\frac{\Delta f}{\epsilon}\right)$ plus « plat »
- bruit plus large
- Bien adapté aux *Counts*



COMPOSITION

Théorème 2.1. (Fermeture sous post-traitement) Soit \mathcal{A} ϵ -DP et soit $f : \mathcal{R} \rightarrow \mathcal{R}$ une fonction arbitraire, indépendante de D . Alors $f \circ \mathcal{A} : D \rightarrow \mathcal{R}$ est ϵ -DP.

Théorème 2.2. (Composition séquentielle) Soient \mathcal{A}_i chacun garantissant la ϵ_i -DP. Une séquence de $\mathcal{A}_i(D)$ sur une base de données D est $(\sum_i \epsilon_i)$ -DP.

Théorème 2.3. (Composition parallèle) Soient \mathcal{A}_i chacun garantissant la ϵ_i -DP. Une séquence de $\mathcal{A}_i(D_i)$ sur des bases de données disjointes D_i est $(\max(\epsilon_i))$ -DP.

COMPOSITION 2

- Les propriétés de composition sont ce pourquoi la DP est devenue un standard *de facto*
 - On peut prouver qu'un algorithme est DP
 - Th2.1 : n'importe quelle fonction appliquée à un mécanisme DP est DP; i.e. on peut publier des données DP sans se soucier des futures analyses à l'inverse du k-anonymat (cf. Capsule prec.)
 - Th2.2 : on peut « découper » ϵ à différentes requêtes séquentielles
 - Th2.3 : on peut borner ϵ lors d'appels à des mécanismes disjoints

LA DP DANS LE MONDE RÉEL

- US Census bureau - résultat des recensements 2020
- Google - outil RAPPOR pour Chrome
- Apple - Statistiques d'usage des macs/iPhones
- Facebook - fourniture de données pour les sciences sociales
- Uber/Amazon/Mozilla/Snapchat
- cont.



PROTECTION DE LA VIE PRIVÉE ET GÉOLOCALISATION

PRÉSENTATIONS PAR ÉQUIPE

OBJECTIFS

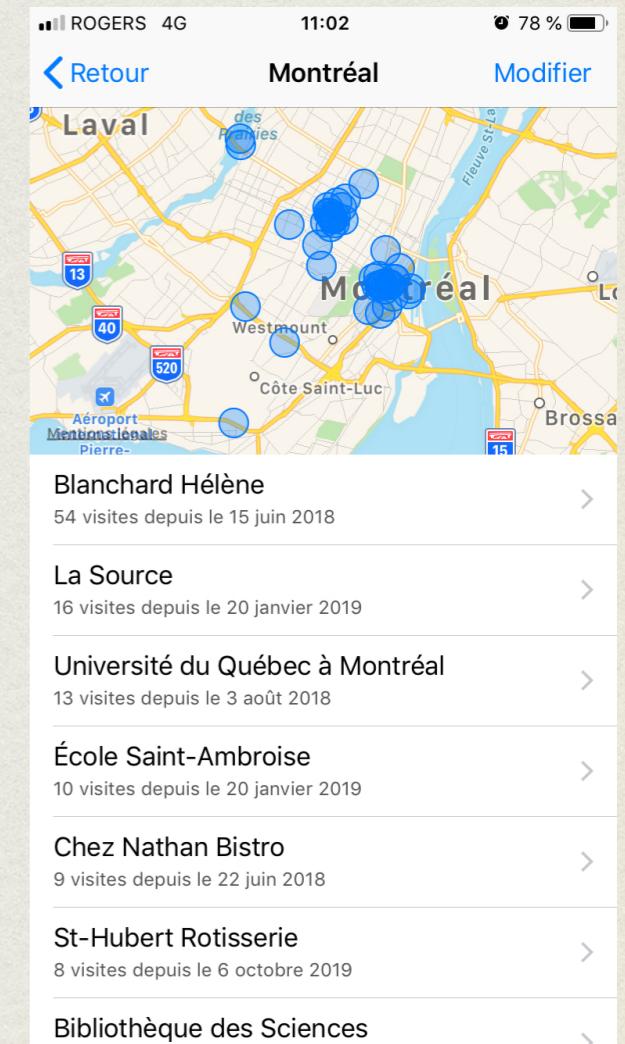
- Chaque équipe doit préparer
 - Une présentation de ~10 min. (ie. des *slides*)
 - A présenter en direct le 19 octobre (*ou en vidéo*)
- Objectifs :
 1. Faire comprendre le sujet avec une *prez* « classique » (~7 min.) = intro, concepts clés, exemples, etc.
 2. En guise de conclusion, discuter des enjeux liés à la sécurité informatique
 - Quels intérêts dans une stratégie de sécurité ?
 - Comment prendre en compte ce sujet, ses concepts, les mécanismes offerts, etc. ?
 - Quels dangers faut-il considérer en termes de sécurité ?

EVALUATION

- Travail d'équipe, note potentiellement individualisée : chaque membre évaluera le travail des autres membres de l'équipe - Obj 0 - « bémols ou dièses »
- Co-évaluation : vous et moi évaluons la présentation
 - Est-ce que j'ai bien compris le sujet ? Obj1 - Lettre - 50%
 - Est-ce que les enjeux de sécurité étaient clairs et bien pris en compte ? Obj 2 - Lettre - 30 %
 - Est-ce que j'ai passé un bon moment en assistant à cette près ? Obj de la vie - Lettre - 20 %

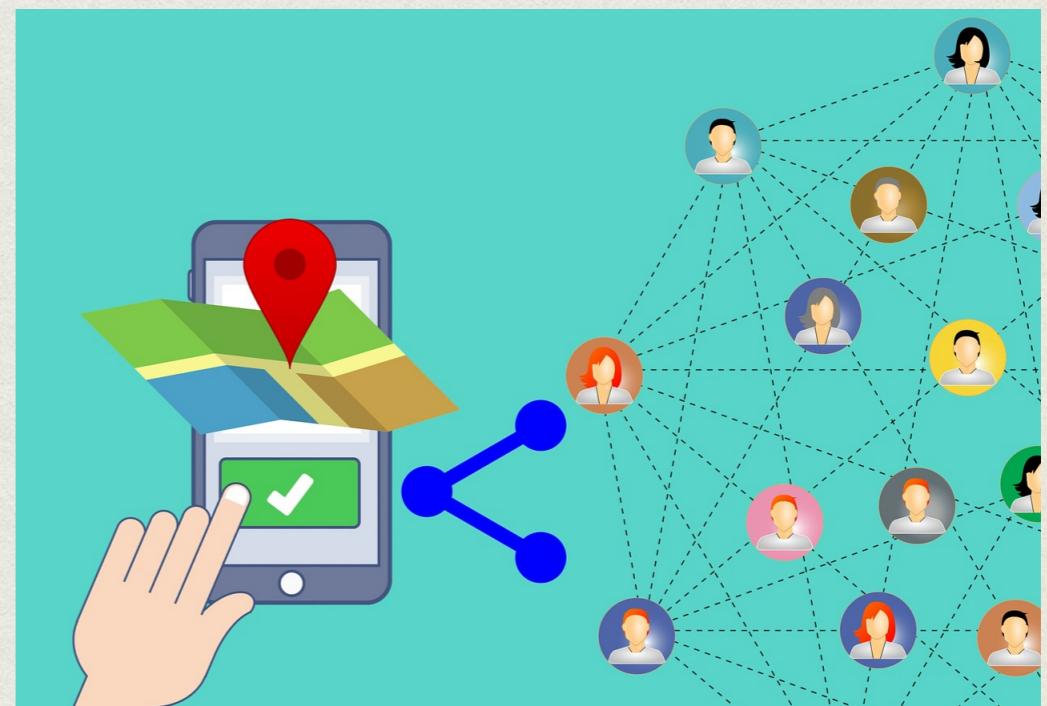
GPS ET GEOLOCALISATION

- On peut inférer tant de chose à partir de votre
 - Compteur électrique
 - Historique de butinage web
 - Compte Facebook
- A partir de votre *Smartphone*, ça donne quoi ?
 - cf. Google Maps Timeline (web ou android)
 - cf. iOS frequent places



GÉOLOCALISATION ?

- La géolocalisation associe une **position géographique** à un objet, souvent personnel
 - et donc la position, in fine, est associé à un individu
 - Si divulguées, peut mener à des bris de vie privée
- **Défi:** concilier usage de géolocalisation et respects de la vie privée



GEOPRIVACY

- *La geoprivacy cherche à empêcher une entité non-désirée d'apprendre la localisation géographique passée, présente et future d'un individu* (Beresford et Strajano 03)
- Les **données personnelles spatio-temporelles** peuvent jouer le rôle d'identifiant (si très précises) ou de quasi-identificateur.
- Permettent **d'inférer**: lieu d'habitation et de travail, identité, centres d'intérêts, habitudes, déviation par rapport au comportement habituel
- Et donc un **bris de vie privée**

DE QUELS SYSTÈMES PARTE T'ON ?

- Téléphone portable, même non intelligent, est localisé par l'opérateur téléphonique pour router les appels (il peut même être triangulé assez précisément)
- Carte de transport (e.g. OPUS) enregistre les points et horaires d'entrée dans le réseau
- Le GPS des autos et téléphones intelligent fournit la position exacte en temps-réel
- L'adresse IP d'un ordinateur peut être reliée à une zone géographique (précision variable)

POUR QUELS SERVICES

- **Communications** téléphoniques et web
- **Statistiques et analyse du trafic** : étude du déplacement de véhicules et/ou de personnes à l'intérieur d'un réseau peut permettre d'analyser sa dynamique et servir à améliorer son efficacité
- **Services géo-localisés** : service adapté à la position géographique de l'utilisateur, e.g. plus proche A&W
- **Urgences** : pour porter secours lors d'un incident, localiser le téléphone (911) ou un dispositif dédié en mer ou montagne (e.g. Argos)



FUITES DE DONNÉES GEOLOCALISÉES

Fabricants de téléphones et d'OS (Apple, Google, MS)

Opérateurs téléphoniques et internet (e.g. Videotron)

Fournisseurs d'applications, de librairies et de services (e.g. Google Maps, Pagesjaunes)

Réseaux sociaux

BDD de recherche (Crawdad)

Fuites de BDD (cf. cours fuites)

The screenshot shows the homepage of pleaserobme.com. At the top, there's a cartoon illustration of a burglar in a mask and a balaclava, carrying a sack, with the text "PLEASE ROB ME" in large red letters next to it. Below the illustration, a map shows several locations marked with red pins, each with a small "X" on it. The main heading reads "Listing all those empty homes out there". A subtext below it says "Check out the same results on [Twitter search](#)". On the left, there's a "Next step" section with a yellow info icon and text about continuing the project. On the right, there's a "More Info" sidebar with links to Home, Why, About, and Made Possible By, which points to [Forthehack](#).

LOCATIONS		
TIME	MEGAN	ROBER
11:00 AM	HOME	
12:30 PM	EASTVIEW ADULT TOY STORE	HOME
1:30 PM	HOME	
2:00 PM	LAKETOWN SEX TOY SHOP	SCHOOL
2:30 PM	HOME	
3:00 PM	FRY'S ELECTRONICS	
3:30 PM	ED'S POWER TOOL EMPORIUM	SUBWAY
4:00 PM	HOME	
4:10 PM	HOSPITAL BURN WARD	

WE'RE IN A NARROW WINDOW IN WHICH PEOPLE ARE USING GOOGLE LATITUDE, BUT HAVEN'T LEARNED THE HABIT OF TURNING IT OFF WHEN THEY'RE DOING SOMETHING DISCREETLY.

I WROTE AN APP TO LOG FRIENDS' LOCATIONS AND WORK OUT ADDRESSES AND BUSINESS NAMES.

A simple cartoon illustration of two stick figures standing and talking. One figure is holding a small device, possibly a phone or a GPS receiver.

OFFRE DE SERVICE (IL-)LÉGALE ?

Alerte sortie de zone géographique



Par SMS, vous paramétrez votre tracker pour qu'il vous envoie une alerte dès que votre véhicule sort d'une zone géographique prédefinie. En cas de sortie de zone, votre tracker vous enverra, par SMS, une alerte en mentionnant :

- Sa position GPS (latitude et longitude)
- Message d'alerte de sortie de zone (**stockade**)
- La date et l'heure
- Sa vitesse de déplacement
- Son niveau de batterie

SMS reçu sur votre portable

Lat : 40.449788 Long : -3.491807
Stockade !
T : 02/02/2010 18:56
Speed : 060
Battery : 68%

Localisation Express'

Protection des personnes



Vous êtes perdu en forêt, blessé, victime d'une agression ?....Pressez pendant 5 secondes le bouton SOS de votre tracker. Tous les numéros de téléphone favoris enregistrés, recevront une alerte par SMS qui mentionne :

- Votre position GPS (latitude et longitude)
- Message d'alerte (**help me !**)
- La date et l'heure
- Votre vitesse de déplacement
- Le niveau de batterie

SMS reçu sur votre portable

Lat : 40.449788 Long : -3.491807
Help me !
T : 02/02/2010 18:56
Speed : 060
Battery : 68%

Localisation Express'

Ecoute des conversations à distance



Votre véhicule a été volé et vous souhaitez écouter ce qu'il se passe ou ce qu'il se dit dans l'environnement de votre tracker ?

Par simple envoi d'un SMS, vous paramétrez à distance votre tracker pour qu'il passe instantanément en mode "écoute à distance".

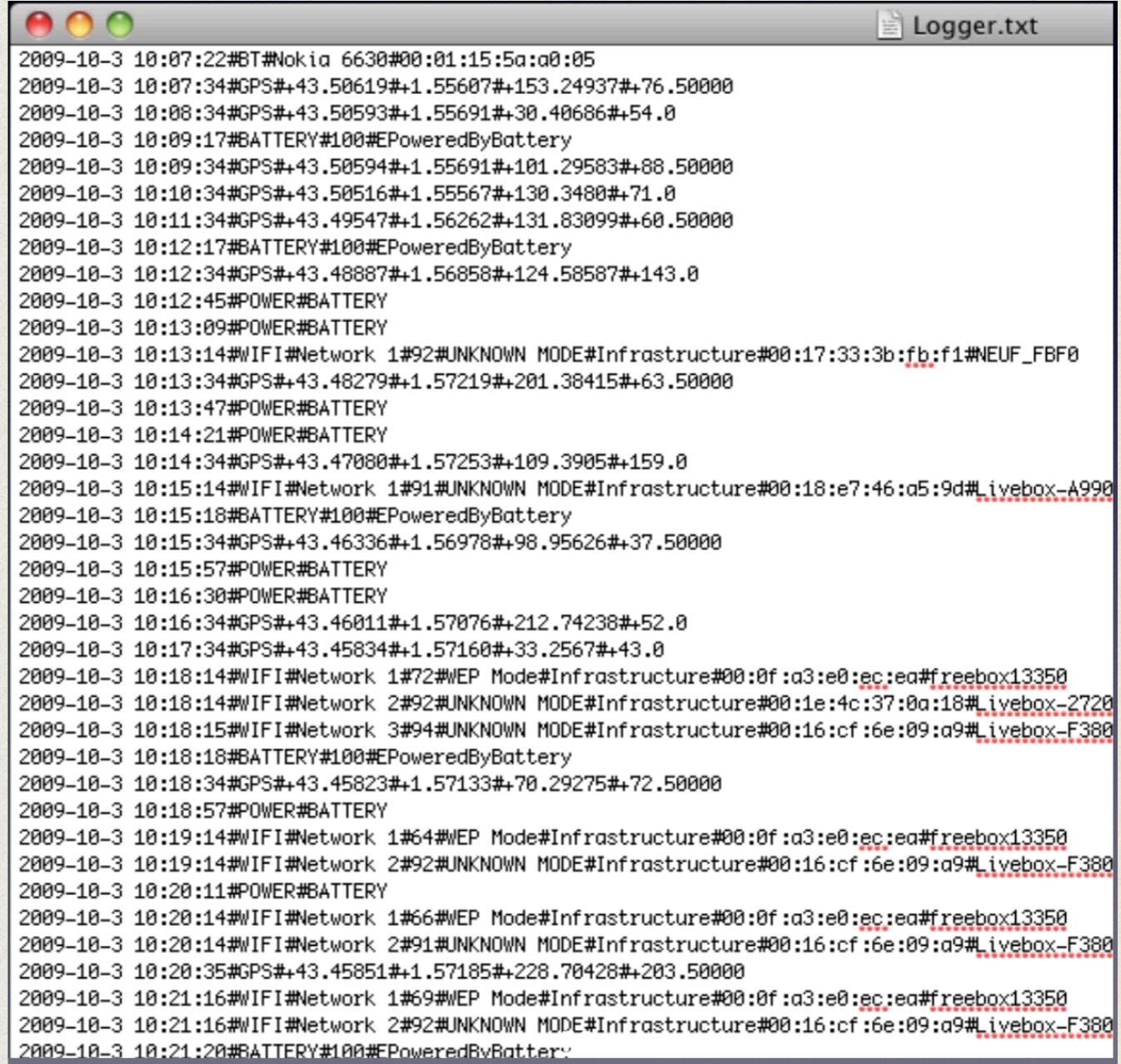
Cette fonction ne doit être utilisée que dans le strict respect de la législation en vigueur sur la vie privée.

Fonction uniquement disponible avec notre tracker "Simply track" !

ATTAQUES DE GÉOPRIVACY

DE QUELLES DONNÉES PARLE T'ON ?

- Hypothèse : l'attaquant dispose des **traces GPS** (lat,lon,alt,date) d'un individu enregistrées sur une certaine période (1j, 1s, 1m, etc.) issues de son téléphone, ou d'une BDD par ex.
- Eventuellement, s'il a accès à son téléphone (pawné), il a **beaucoup plus** : les SSID WiFi et les dispositifs BT rencontrés, les appels et textos émis/reçus, l'état de la batterie, etc.



The screenshot shows a window titled "Logger.txt" displaying a log of device events. The log entries are timestamped and include various types of data such as GPS coordinates, battery levels, power status, and network information. Some entries are redacted with dotted lines.

```
2009-10-3 10:07:22#BT#Nokia 6630#00:01:15:5a:a0:05
2009-10-3 10:07:34#GPS#+43.50619#+1.55607#+153.24937#+76.50000
2009-10-3 10:08:34#GPS#+43.50593#+1.55691#+30.40686#+54.0
2009-10-3 10:09:17#BATTERY#100#EPoweredByBattery
2009-10-3 10:09:34#GPS#+43.50594#+1.55691#+101.29583#+88.50000
2009-10-3 10:10:34#GPS#+43.50516#+1.55567#+130.3480#+71.0
2009-10-3 10:11:34#GPS#+43.49547#+1.56262#+131.83099#+60.50000
2009-10-3 10:12:17#BATTERY#100#EPoweredByBattery
2009-10-3 10:12:34#GPS#+43.48887#+1.56858#+124.58587#+143.0
2009-10-3 10:12:45#POWER#BATTERY
2009-10-3 10:13:09#POWER#BATTERY
2009-10-3 10:13:14#WIFI#Network 1#92#UNKNOWN MODE#Infrastructure#00:17:33:3b:fb:f1#NEUF_FBF0
2009-10-3 10:13:34#GPS#+43.48279#+1.57219#+201.38415#+63.50000
2009-10-3 10:13:47#POWER#BATTERY
2009-10-3 10:14:21#POWER#BATTERY
2009-10-3 10:14:34#GPS#+43.47080#+1.57253#+109.3905#+159.0
2009-10-3 10:15:14#WIFI#Network 1#91#UNKNOWN MODE#Infrastructure#00:18:e7:46:a5:9d#Livebox-A990
2009-10-3 10:15:18#BATTERY#100#EPoweredByBattery
2009-10-3 10:15:34#GPS#+43.46336#+1.56978#+98.95626#+37.50000
2009-10-3 10:15:57#POWER#BATTERY
2009-10-3 10:16:30#POWER#BATTERY
2009-10-3 10:16:34#GPS#+43.46011#+1.57076#+212.74238#+52.0
2009-10-3 10:17:34#GPS#+43.45834#+1.57160#+33.2567#+43.0
2009-10-3 10:18:14#WIFI#Network 1#72#WEP Mode#Infrastructure#00:0f:a3:e0:ec:ea#freebox13350
2009-10-3 10:18:14#WIFI#Network 2#92#UNKNOWN MODE#Infrastructure#00:1e:4c:37:8a:18#Livebox-2720
2009-10-3 10:18:15#WIFI#Network 3#94#UNKNOWN MODE#Infrastructure#00:16:cf:6e:09:a9#Livebox-F380
2009-10-3 10:18:18#BATTERY#100#EPoweredByBattery
2009-10-3 10:18:34#GPS#+43.45823#+1.57133#+70.29275#+72.50000
2009-10-3 10:18:57#POWER#BATTERY
2009-10-3 10:19:14#WIFI#Network 1#64#WEP Mode#Infrastructure#00:0f:a3:e0:ec:ea#freebox13350
2009-10-3 10:19:14#WIFI#Network 2#92#UNKNOWN MODE#Infrastructure#00:16:cf:6e:09:a9#Livebox-F380
2009-10-3 10:20:11#POWER#BATTERY
2009-10-3 10:20:14#WIFI#Network 1#66#WEP Mode#Infrastructure#00:0f:a3:e0:ec:ea#freebox13350
2009-10-3 10:20:14#WIFI#Network 2#91#UNKNOWN MODE#Infrastructure#00:16:cf:6e:09:a9#Livebox-F380
2009-10-3 10:20:35#GPS#+43.45851#+1.57185#+228.70428#+203.50000
2009-10-3 10:21:16#WIFI#Network 1#69#WEP Mode#Infrastructure#00:0f:a3:e0:ec:ea#freebox13350
2009-10-3 10:21:16#WIFI#Network 2#92#UNKNOWN MODE#Infrastructure#00:16:cf:6e:09:a9#Livebox-F380
2009-10-3 10:21:20#BATTERY#100#EPoweredByBattery
```

OBJECTIFS D'ATTAQUE

1. Identifier des points d'intérêts
2. Prédire les déplacements
3. Apprendre la sémantique des localisations et des mouvements
4. Dé-anonymiser des données géolocalisées
5. Chaîner un individu dans différentes bases de données
6. Reconstruire un réseau social
7. Prédire des attributs démographiques

CONNAISSANCES AUXILIAIRES

L'adversaire a souvent accès à des connaissances auxiliaires qui l'aident dans ses attaques

- **présence dans une BDD anonymisée**, e.g. à partir d'une attaque préalable ou ingénierie sociale
- connaissance partielle d'**attributs personnels** (@domicile et/ou lieu de travail) e.g. à partir de réseaux sociaux
- modèle de ses **habitudes**, e.g. suivi (*spying/stalking*) dans la vie réelle
- connaissance de son **réseau social**
- connaissance de la distribution d'**attributs démographiques** de la population globale et/ou connaissance de l'appartenance d'un groupe social/ethnique/particulier
- connaissance **géographique** des routes et du relief
- ...

OBJECTIFS D'ATTAQUE

- 1. Identifier des points d'intérêts**
- 2. Prédire les déplacements**
- 3. Apprendre la sémantique des localisations et des mouvements**
- 4. Dé-anonymiser des données géolocalisées**
- 5. Chaîner un individu dans différentes bases de données**
- 6. Reconstruire un réseau social**
- 7. Prédire des attributs démographiques**

POINTS D'INTÉRÊTS

- **POI** : un site ou un point digne d'intérêt pour un individu (domicile, lieu de travail, ...) ou un groupe d'individus (panorama, boulangerie, stations de métro,...)
- Identifié par sa **position** (*lat,lon*), éventuellement avec une **étiquette sémantique**
- Obtenu de différentes façons :
 - une BDD (connaissance externe) : ex. OpenMaps
 - par questionnaire : où habitez/travaillez vous ?
 - heuristiques à partir de données de localisation
 - attaques d'inférence (clustering, etc.)

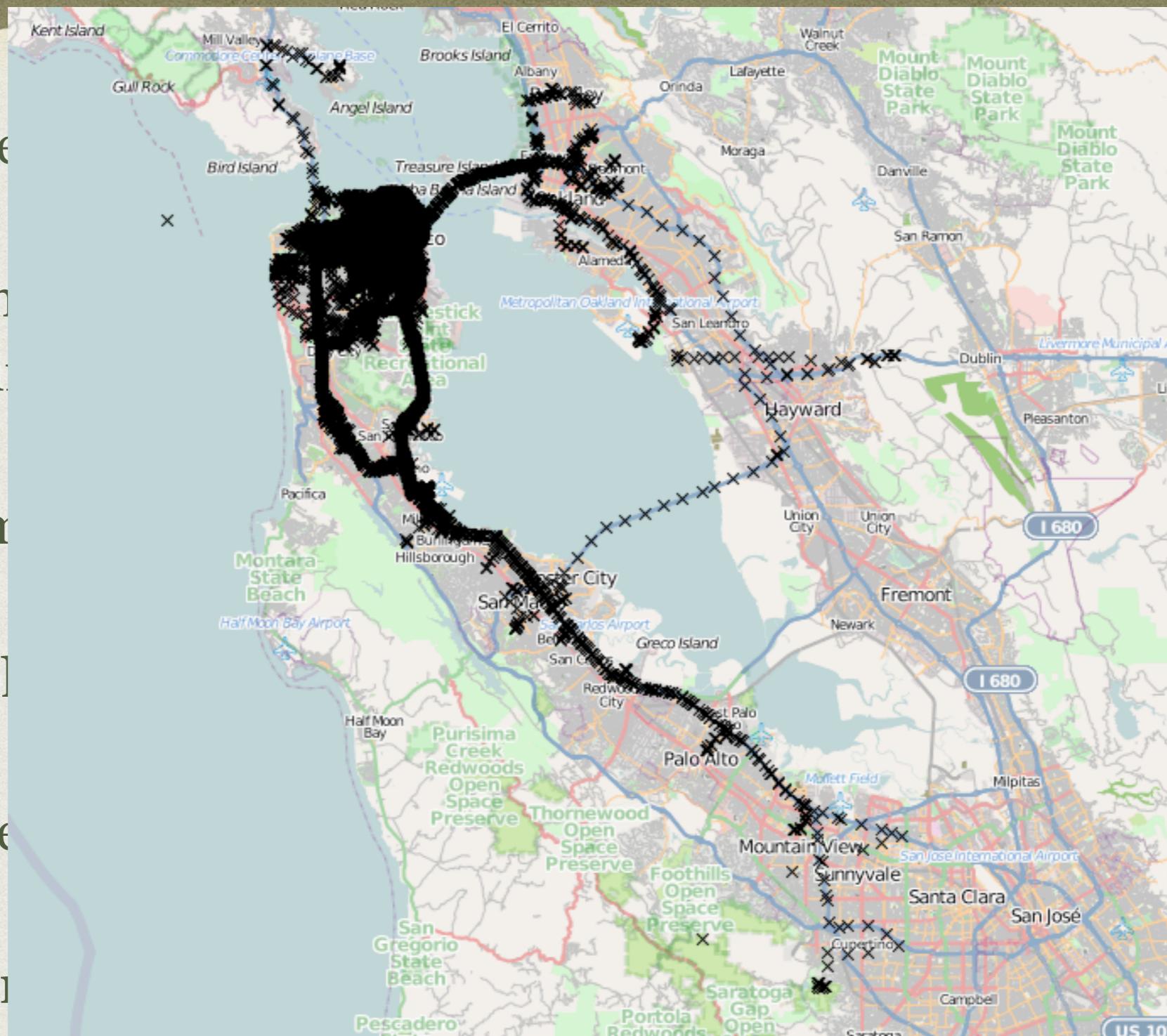


HEURISTIQUE SIMPLE

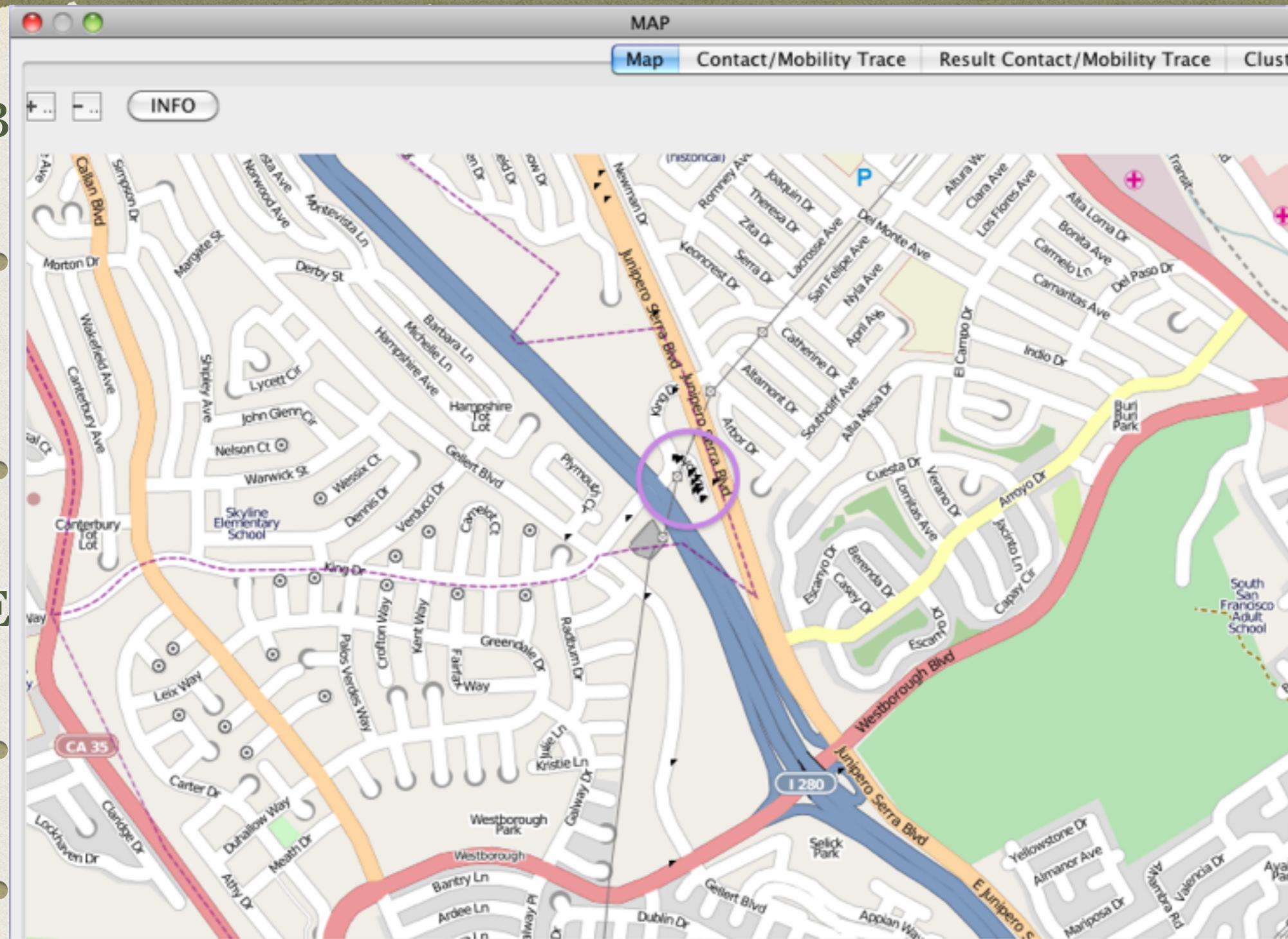
- Begin/end
 - La mobilité quotidienne commence/s'arrête souvent au domicile
 - Premier/dernier point de la journée -> domicile
- Exemple d'application à 90 taxis de San Francisco [Données Crawdad]
 - 30 se parquent à la compagnie
 - 20 en zone résidentielle

HEURISTIQUES SIMPLE

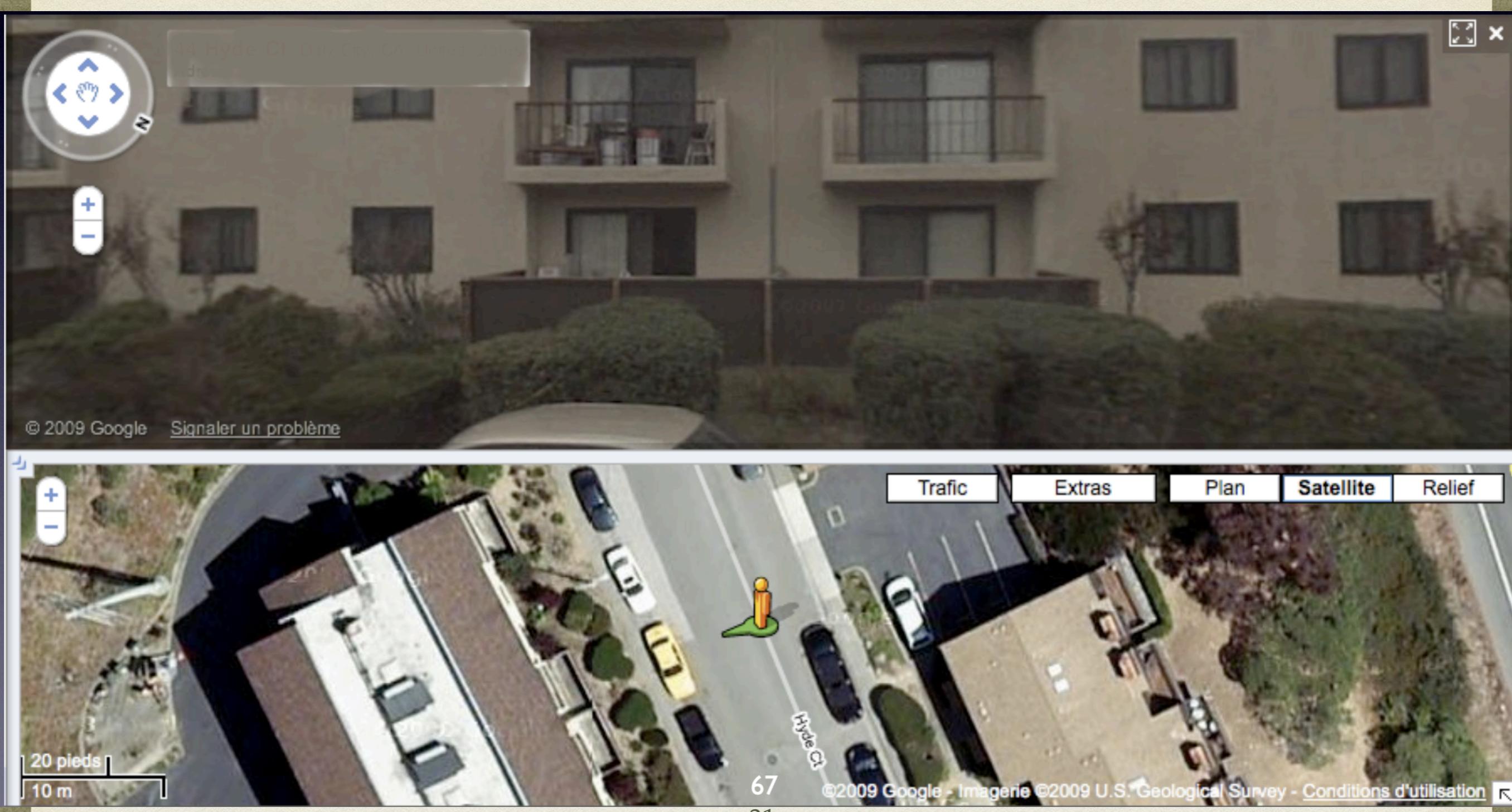
- Begin/end point
- La meilleure solution au domino
- Première solution
- Exemples
 - 30 secondes
 - 20 en 10 minutes



HEURISTIQUES SIMPLE



HEURISTIQUES SIMPLE



HEURISTIQUE SIMPLE

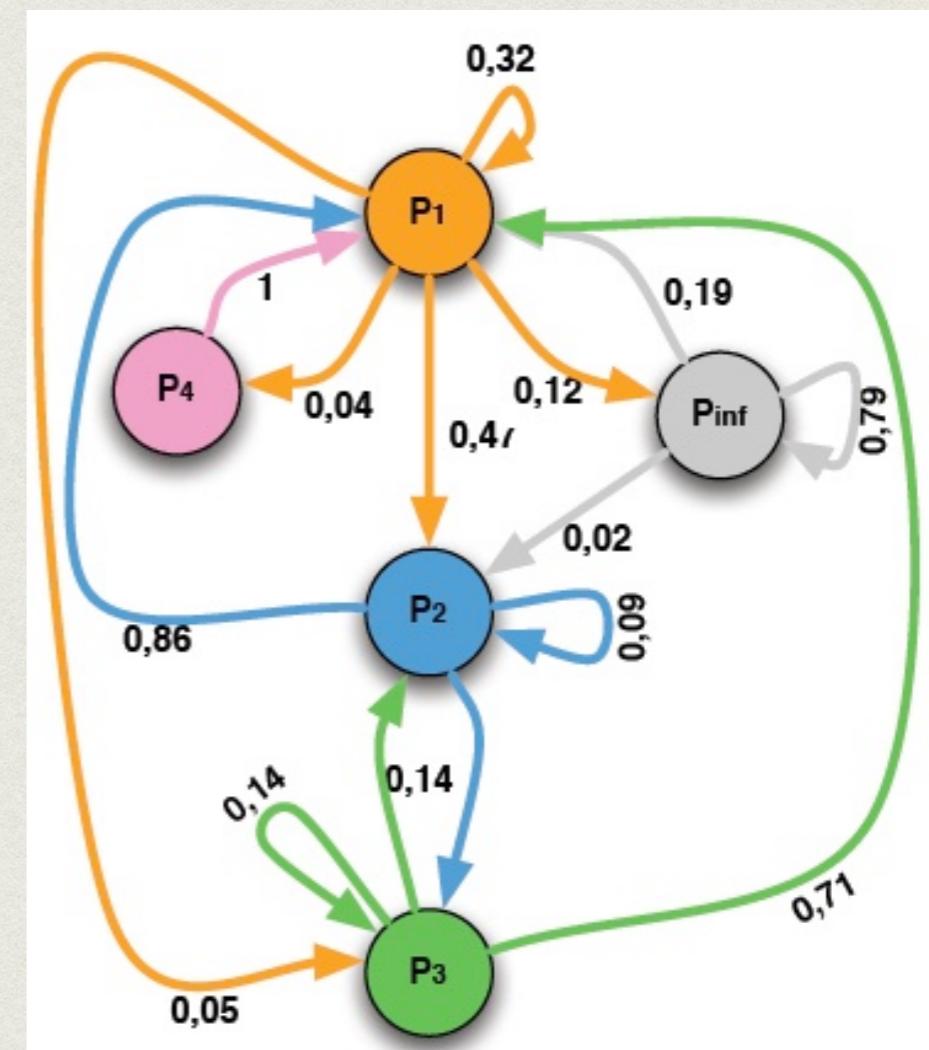
- Les humains sont prévisibles (au moins dans leur mobilité)
- Il existe donc une infinité d'heuristiques possibles, par exemple :
 - Lieu de travail : l'endroit où il y a le moins de déplacement dans la journée (entre 9h et 17h)
 - Magasinage : l'endroit où il y a un arrêt le soir entre le lieu de travail et le domicile
 - etc.

OBJECTIFS D'ATTAQUE

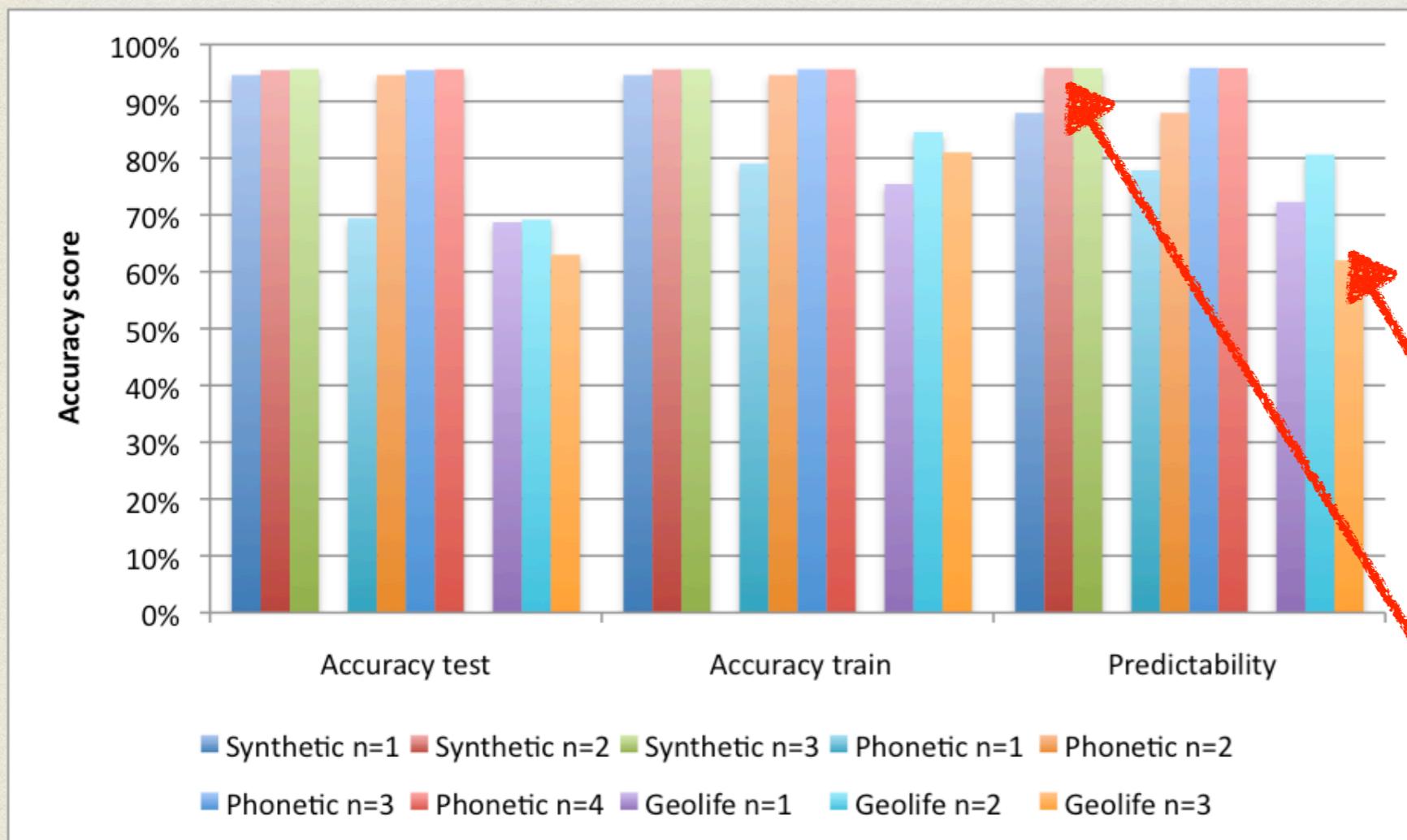
1. Identifier des points d'intérêts
- 2. Prédire les déplacements**
3. Apprendre la sémantique des localisations et des mouvements
4. Dé-anonymiser des données géolocalisées
5. Chaîner un individu dans différentes bases de données
6. Reconstruire un réseau social
7. Prédire des attributs démographiques

MODÉLISER LA MOBILITÉ D'UN INDIVIDU

- Différentes formes possibles : graphes pondérés, chaînes de Markov, etc.
 - états = POIs
 - arrêtes = transitions entre les POIs
 - poids = probabilité de passer d'un POI à un autre
- Calculés simplement :
 - Identification des POIs par **clustering** (K-means ou DB-scan par ex.)
 - Calcul des poids des transition par **mesure des probabilités** dans les traces
 - On enlève les traces « non-POI » et on compte les transitions puis on normalise
- Modèle de la **mobilité passée** qui peut être utilisé pour la prédiction de la **mobilité future**
 - POI le plus probable** à partir de la position actuelle



MODÉLISER LA MOBILITÉ D'UN INDIVIDU



Selon le jeu de données et la paramétrisation de l'attaque, succès

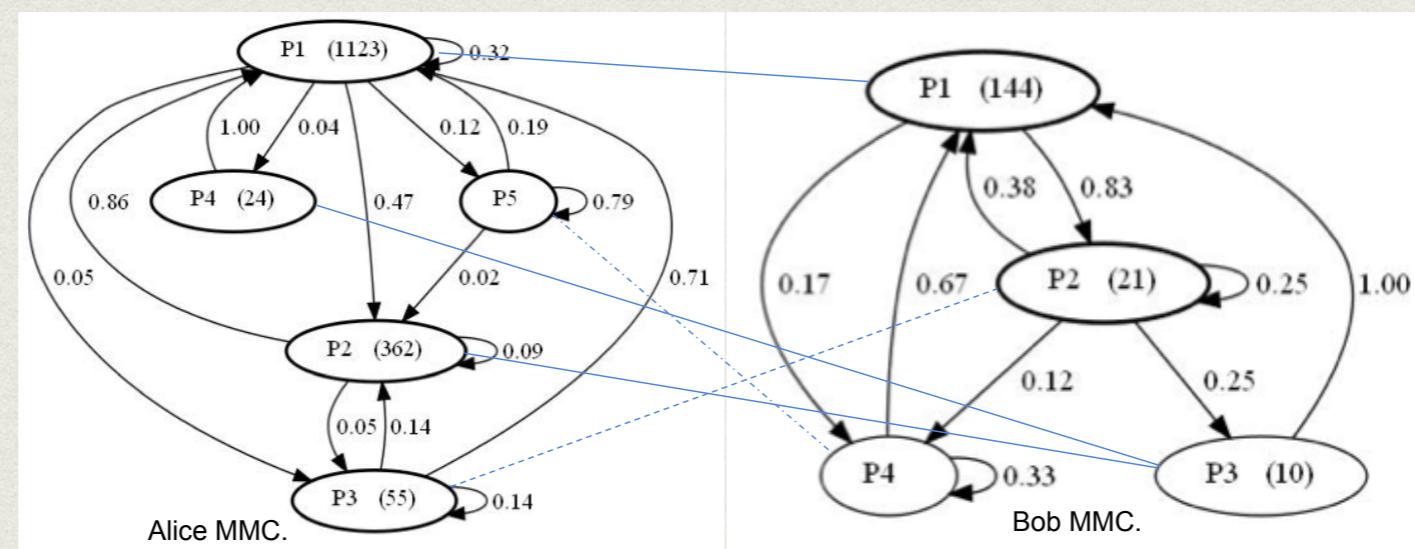
entre 60%
et 95%

OBJECTIFS D'ATTAQUE

1. Identifier des points d'intérêts
2. Prédire les déplacements
3. Apprendre la sémantique des localisations et des mouvements
4. Dé-anonymiser des données géolocalisées
- 5. Chaîner un individu dans différentes bases de données**
6. Reconstruire un réseau social
7. Prédire des attributs démographiques

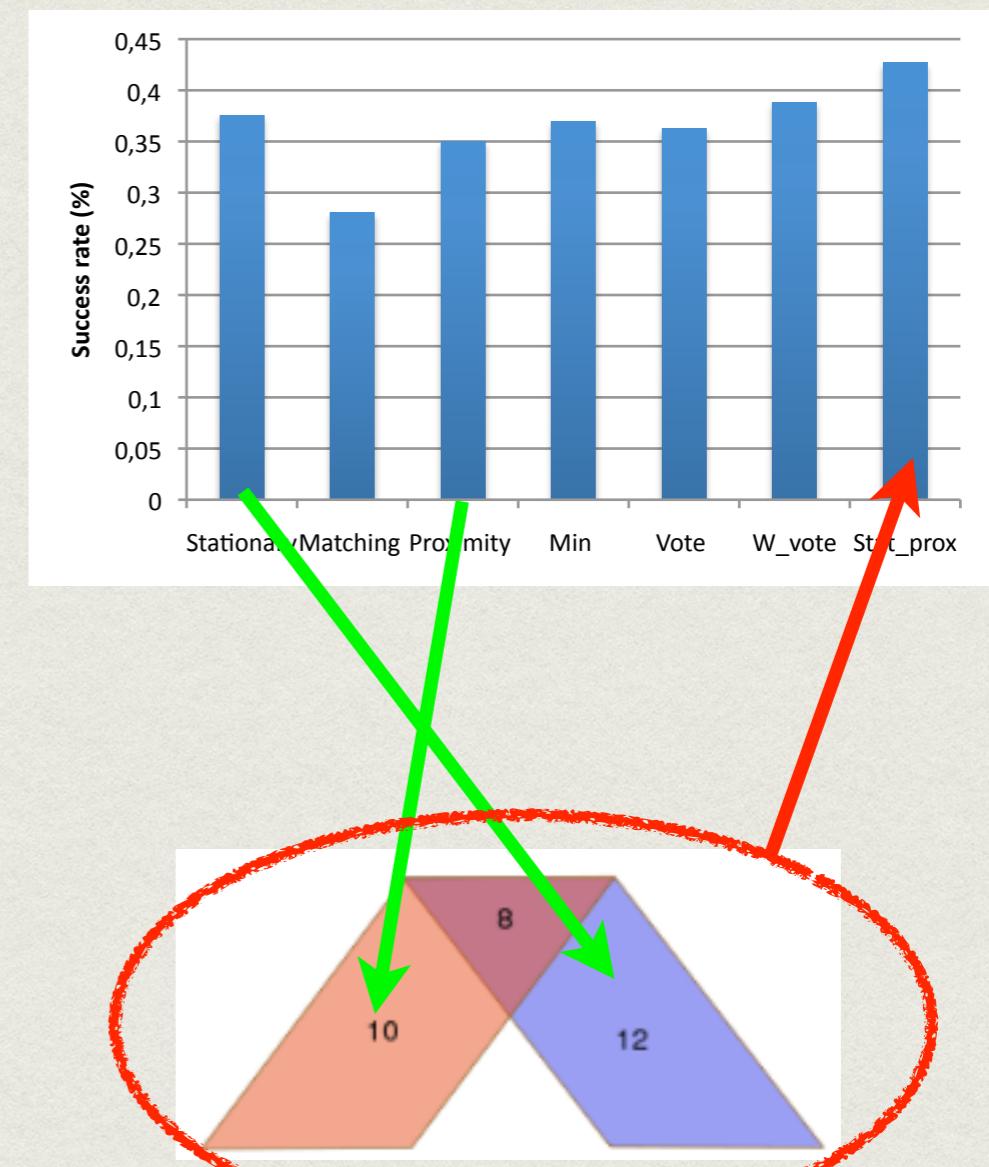
ATTAQUE PAR CHAINAGE DE MOBILITÉ

- Eve connaît la (chaine de Markov de) mobilité d'Alice
- Eve veut savoir si Alice est dans une BDD anonymisée, et si oui connaître son profil
 1. Calcul des **modèles** pour la BDD anonymisée
 2. Calcul des **distances** entre les modèles d'Alice et de la BDD
 3. **Choisit** le modèle « le plus proche »



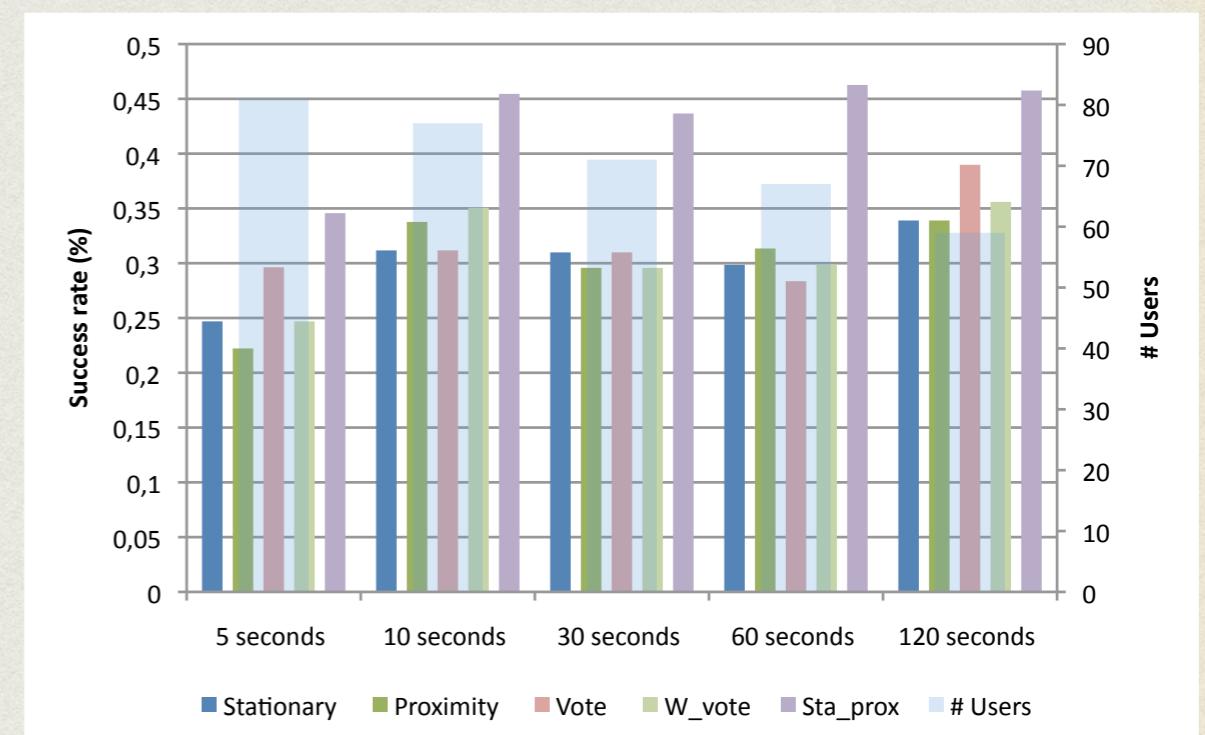
DIFFICULTÉ DE DÉFINIR UNE DISTANCE

- Il n'y a pas de distance parfaite (connue) entre 2 modèles
- Différentes distances donnent des résultats différents et parfois complémentaires
- Les distances peuvent être combinées entre elles



CA MARCHE ?

- Non seulement ça fonctionne avec des taux de succès proche de 45%
- Mais c'est robuste à l'assainissement de la BDD
- Car l'homme est prévisible : **boulot-métro-dodo**
- En confinement CoVid c'est pire : maison-dépanneur-épicerie



OBJECTIFS D'ATTAQUE

- 1. Identifier des points d'intérêts**
- 2. Prédire les déplacements**
3. Apprendre la sémantique des localisations et des mouvements
4. Dé-anonymiser des données géolocalisées
- 5. Chaîner un individu dans différentes bases de données**
6. Reconstruire un réseau social
7. Prédire des attributs démographiques

OBJECTIFS D'ATTAQUE

1. Identifier des points d'intérêts

Alice+Map

2. Prédire les déplacements

3. Apprendre la sémantique des localisations et des mouvements

4. Dé-anonymiser des données géolocalisées

POIs+Aux

5. Chaîner un individu dans différentes bases de données

6. Reconstruire un réseau social

Alice+Bob+Charlie

7. Prédire des attributs démographiques

Alice+Aux

OBJECTIFS D'ATTAQUE

1. Identifier des points d'intérêts
2. Prédire les déplacements
3. Apprendre la sémantique des localisations et des mouvements
4. Dé-anonymiser des données géolocalisées
5. Chaîner un individu dans différentes bases de données
6. Reconstruire un réseau social
7. **Prédire des attributs démographiques**

HAPPY HOUR ?



Macrosense

Citysense

Technology

Principles

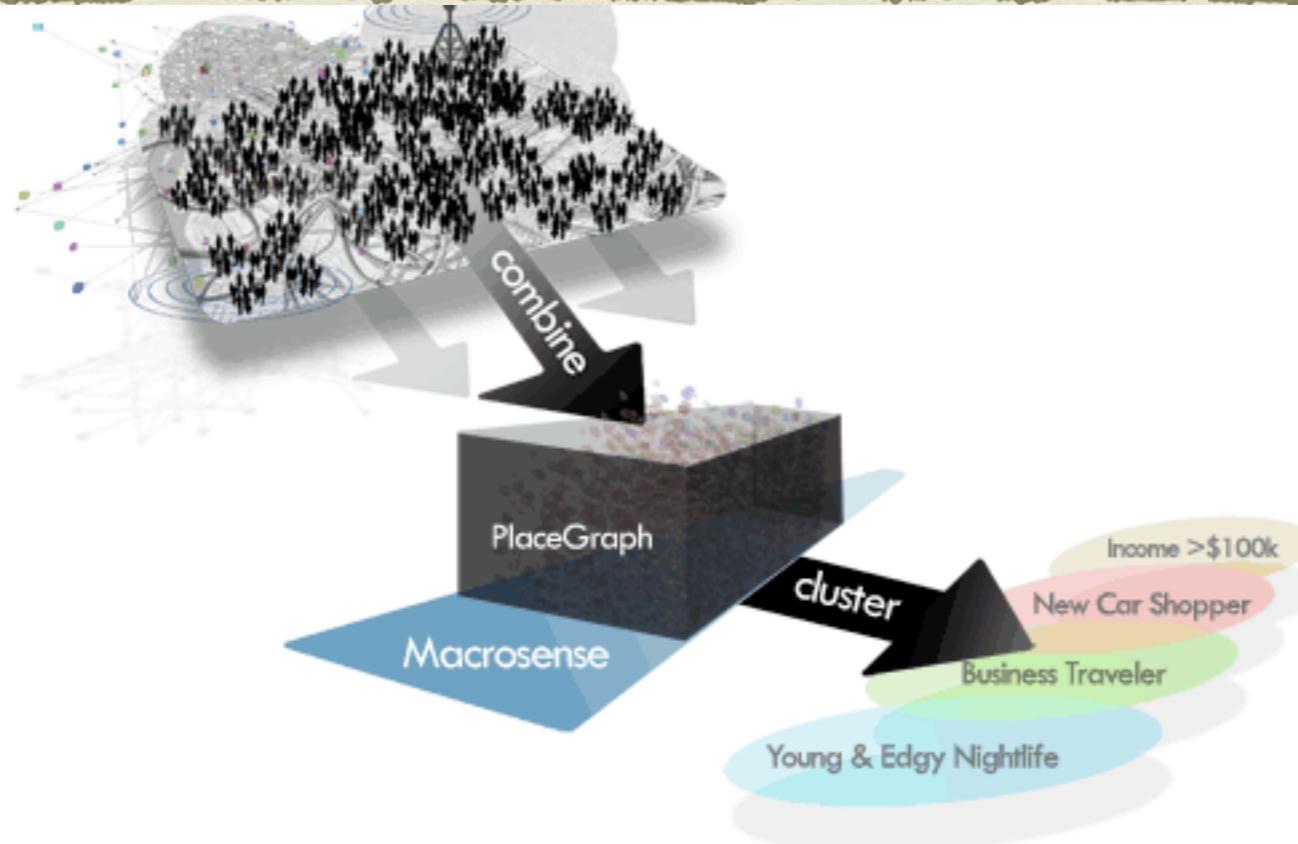
Media Center

About Us



**Indexing the real world using location data
for predictive analytics.**

OUI MAIS PAS POUR CELUI QUE TU PENSES !



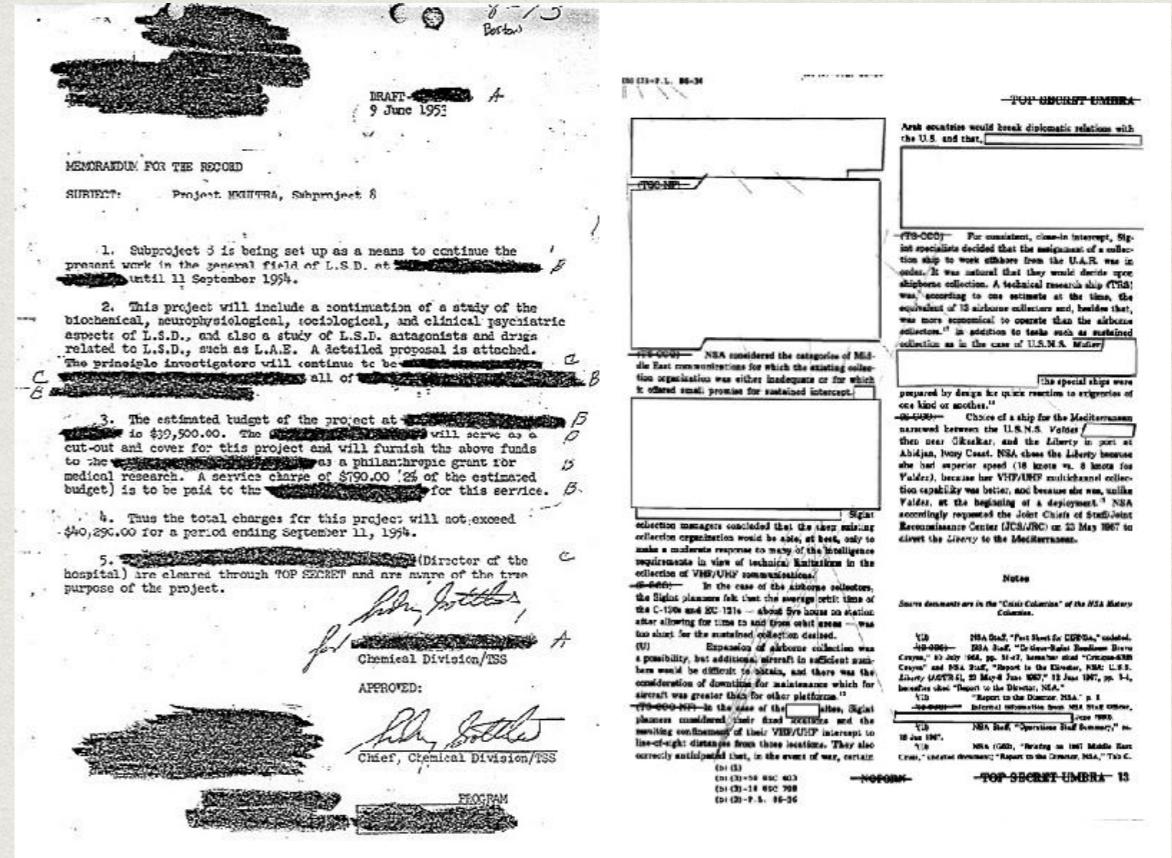
Macrosense enables companies to:

- Better understand customers using existing data, without requiring any change in behavior
- Segment and cluster customers into marketing groups based on actual unbiased behavior with unprecedented accuracy and relevance
- Personalize recommendations and advertisements based on popularity with "people like me"
- Automatically find and present the most relevant suggestions to a particular audience
- Identify group influencers

PROTECTION DE LA GÉOPRIVACY

ASSAINISSEMENT DE DONNÉES ?

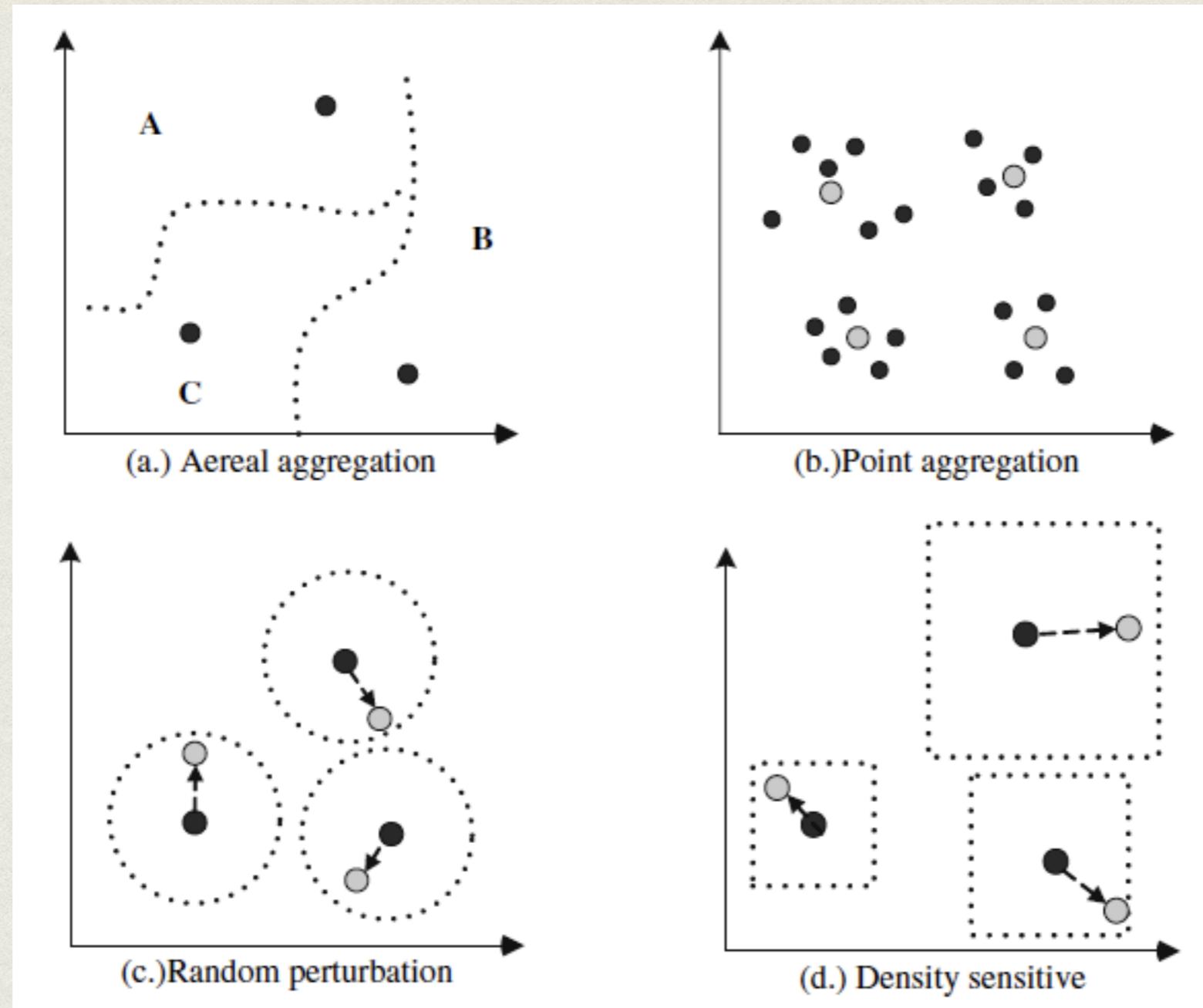
- (Sanitization en anglais)
- Accroître l'incertitude dans les données
- Compromis entre le niveau de protection désiré et la qualité des données assainies (utilité)



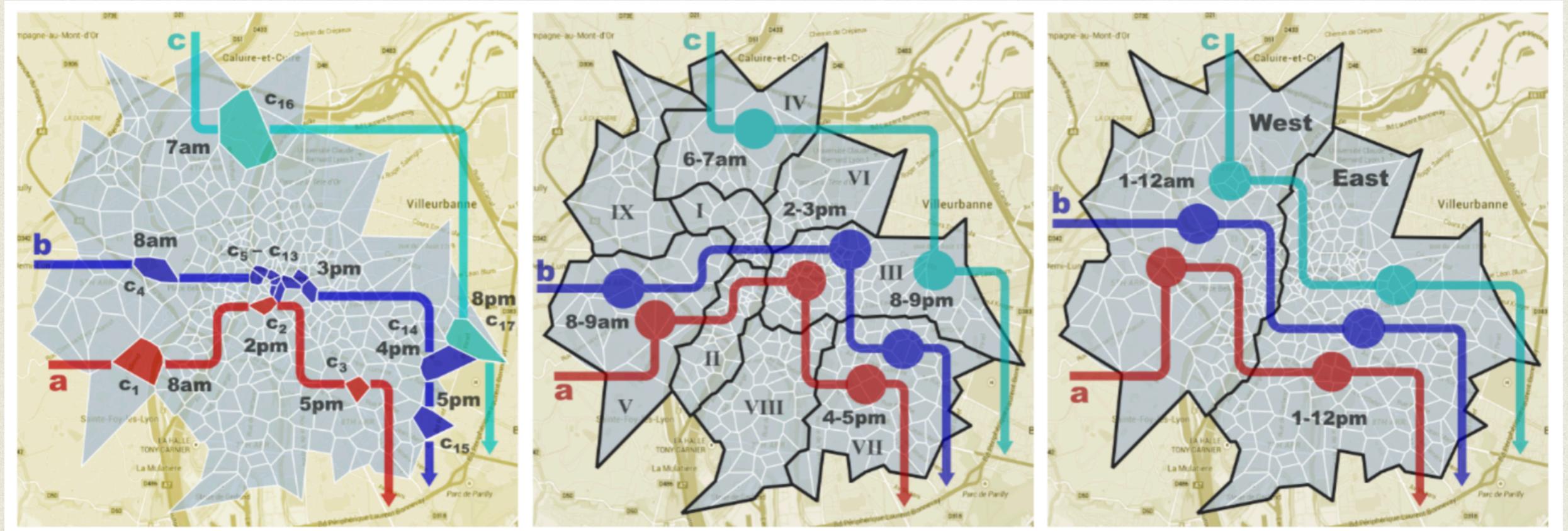
MASQUES GÉOGRAPHIQUES

- Modifier la localisation afin de préserver la vie privée
 - **Agrégation** de la localisation d'un ou plusieurs individus en une zone ou une position (par ex. la moyenne ou médiane)
 - **Perturbation** aléatoire (par ex. tirer une direction et une distance)
 - **Randomisation** en tenant compte de la densité dans la zone (zone dense, faible perturbation ; zone peu dense, forte perturbation)

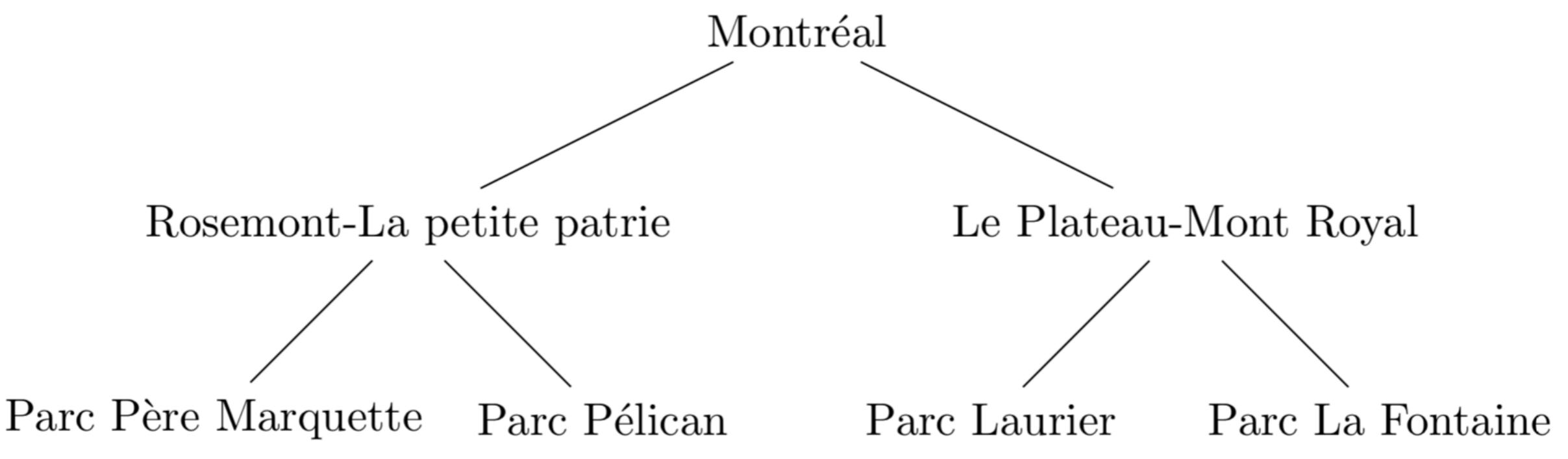
EXEMPLES DE MASQUES



AGRÉGATION SPATIO-TEMPORELLE



AGRÉGATION SÉMANTIQUE

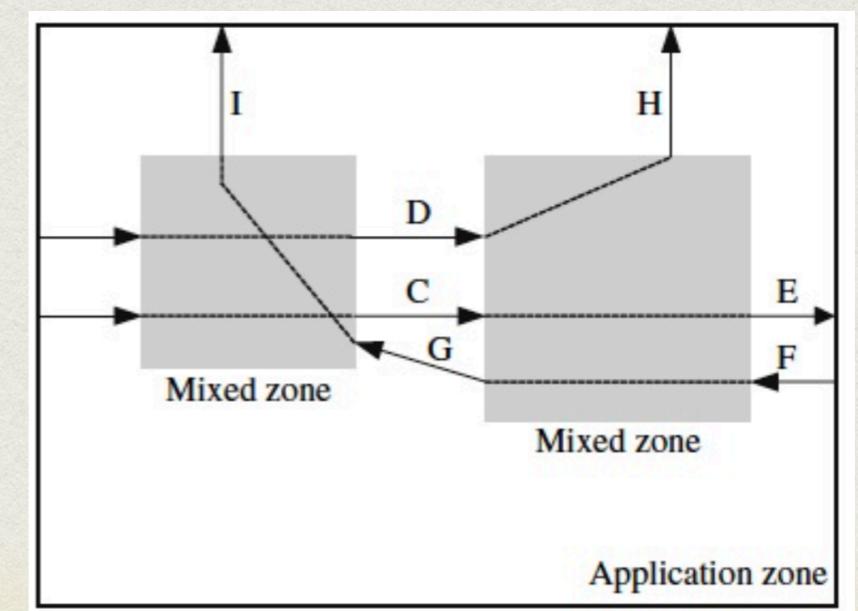
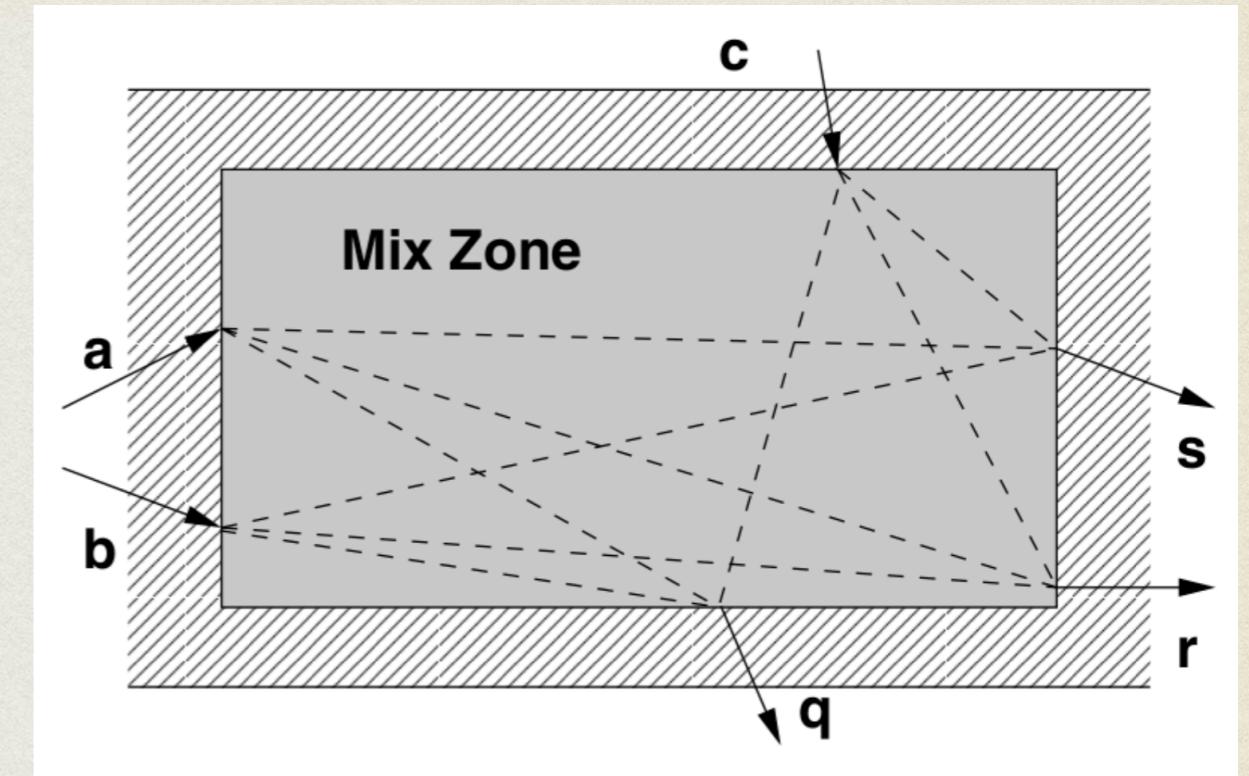


AUTRES TRANSFORMATIONS POSSIBLES

- **Echantillonner** avec une fréquence moindre
- **Echanger** les traces de deux individus
- **Enlever** des positions trop sensibles
- **Ajouter** de faux enregistrements ou de faux individus
- *Science-presque-fiction* : apprendre un **modèle génératif** de la mobilité des individus de la BDD et **générer de nouvelles traces** qui ont de bonnes propriétés mais qui ne correspondent pas à des mobilités réelles

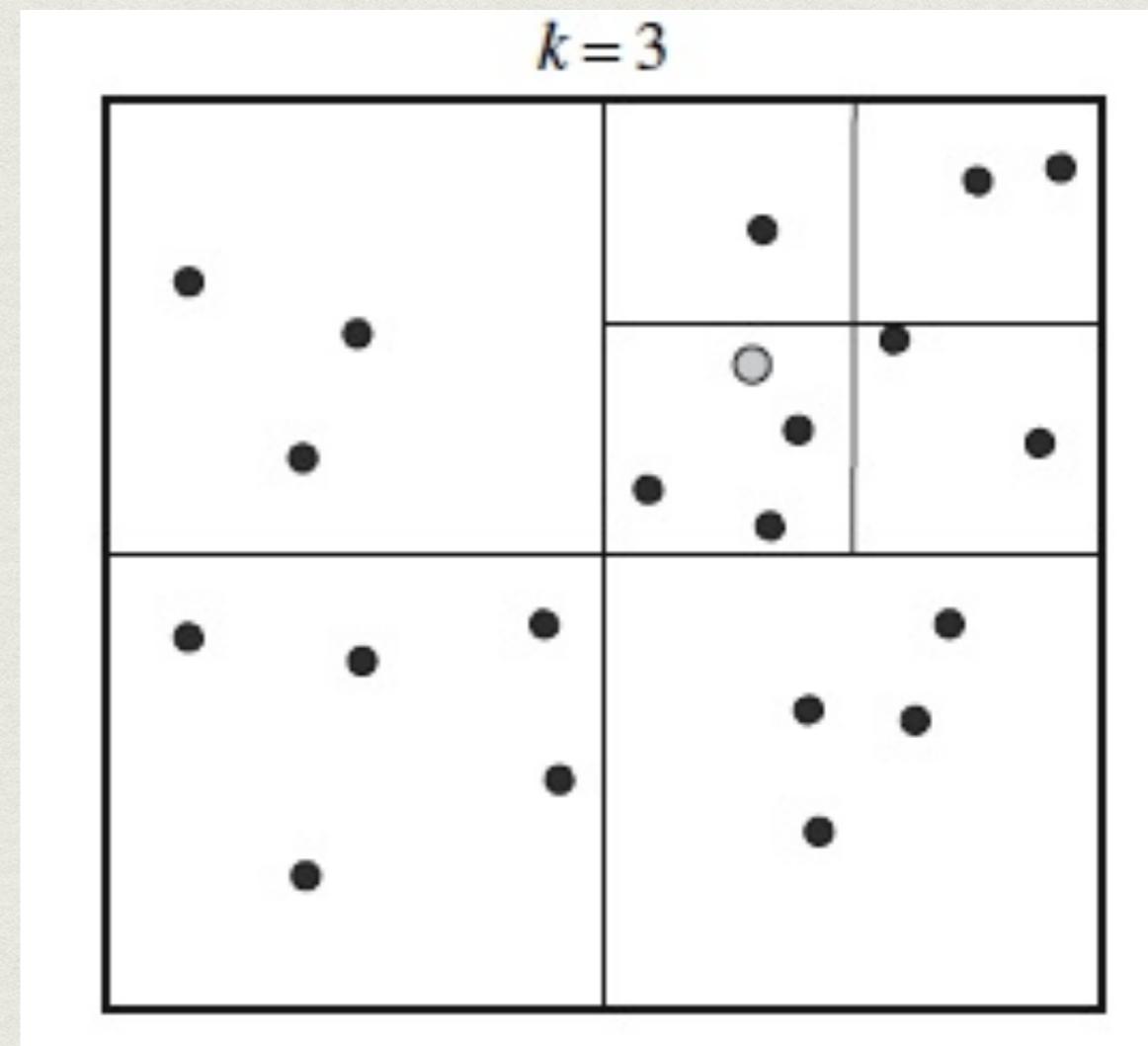
MIX-ZONES

- Sur la base des Mix-nets, les zones de mixage
 - non-chaînabilité entre zones
 - des zones où aucune localisation n'est enregistrée
 - changement de pseudonyme qd on en sort
- Besoin d'entropie donc pb si :
 - majorité des traces ont le même parcours
 - une seule trajectoire passe par une zone
- Le choix des zones est primordial



K-ANONYMAT GÉOGRAPHIQUE ?

- Couverture spatiale : extension du k-anonymat aux données spatio-temporelles
- A chaque unité de temps, chaque individu est dans une zone partagée par au moins $k-1$ autres individus
- Par ex. découper récursivement l'espace

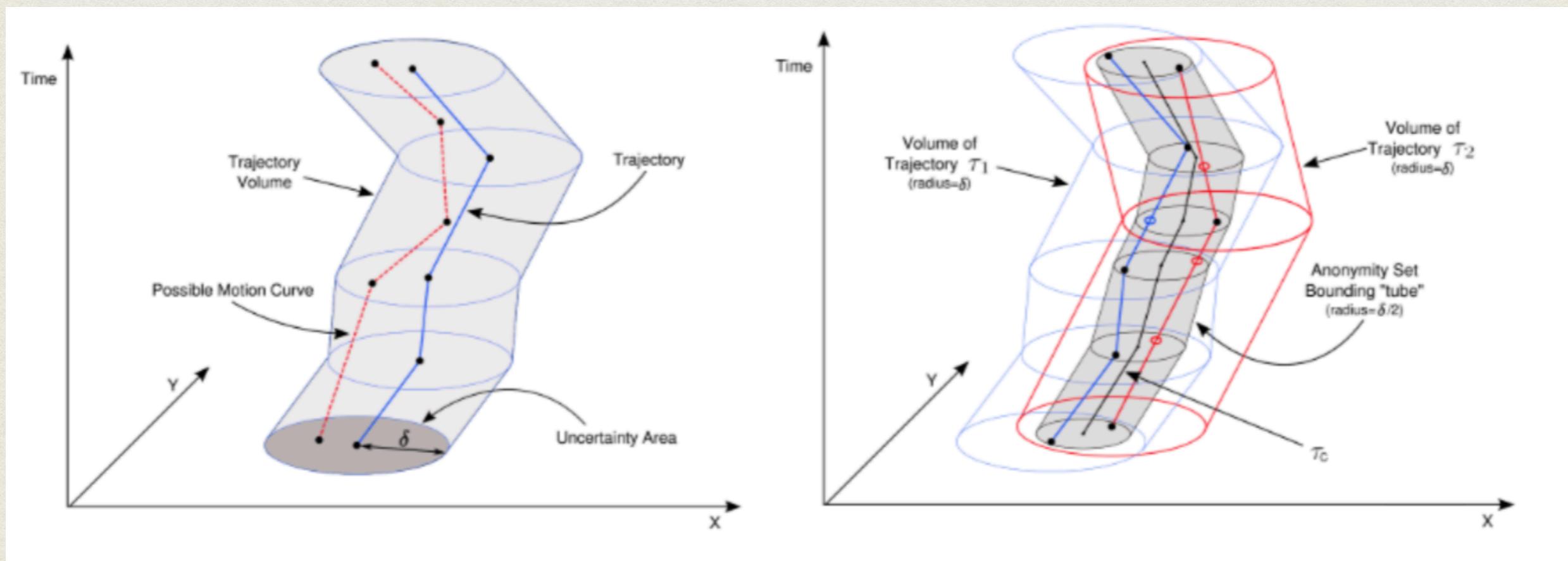


LIMITES DES MASQUES ET COUVERTURE SPATIALE

- En fonction des connaissances aux. de l'adv. attaques possible :
 - **Connaissance géographiques** : écarter certaines hypothèses peu probables
 - Par ex. suite à perturbation aléatoire la localisation est difficilement accessible (milieu du St Laurent), cette hypothèse est écartée à la faveur de la zone la plus proche
 - **Chainabilité**: il est parfois possible de chainer les actions d'un groupe d'individu

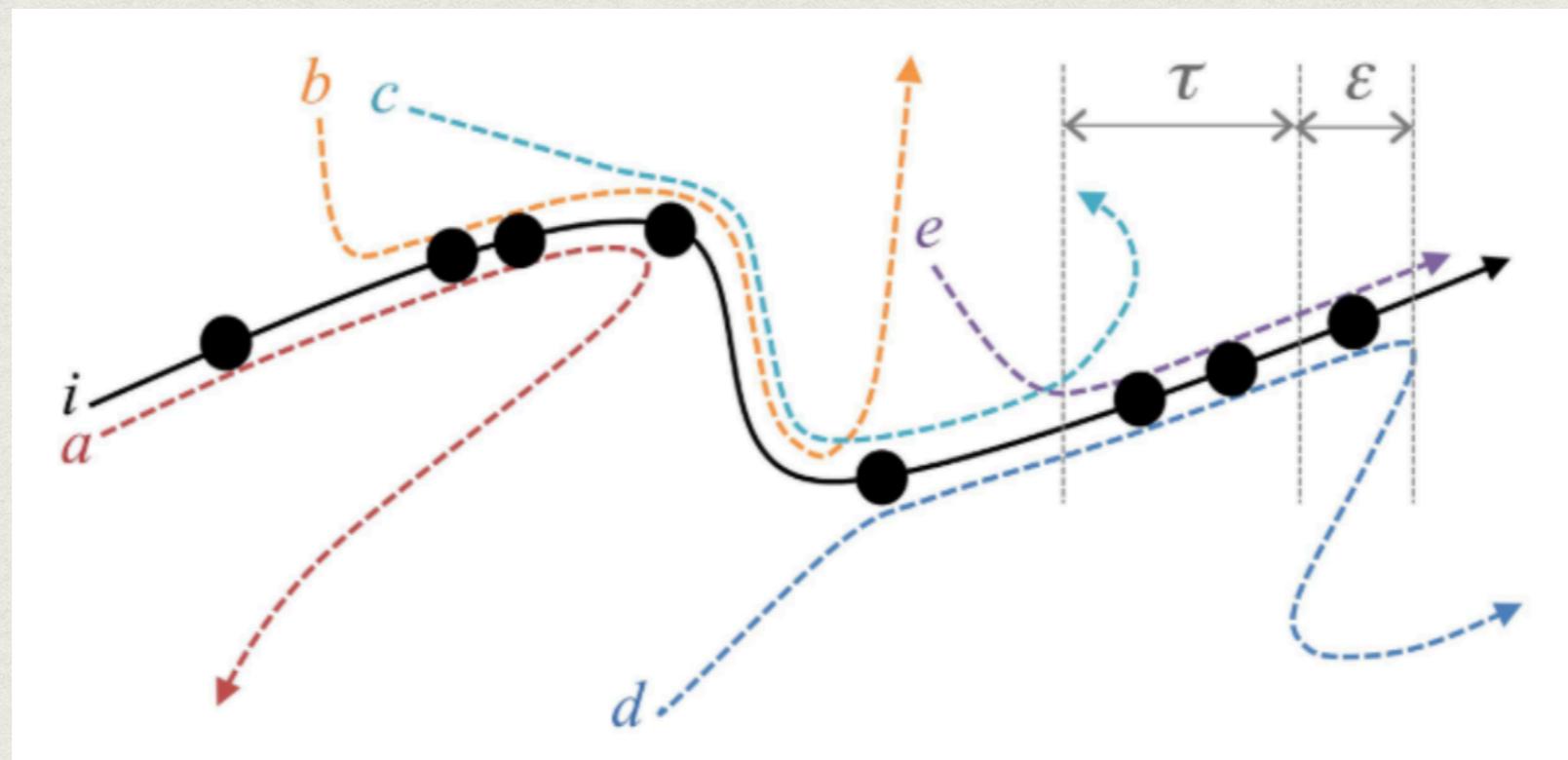
(k, δ) -ANONYMAT

- Les trajectoires doivent se trouver au plus à une distance δ de $k-1$ autres trajectoires



$k^{\tau,\epsilon}$ -ANONYMAT

- Un adversaire qui observe la trajectoire pendant une durée τ (le passé) et possède une capacité d'inférence ϵ (le futur) est incapable de la distinguer de k trajectoires



LIMITES DU K-ANONYMAT (ET VARIANTES)

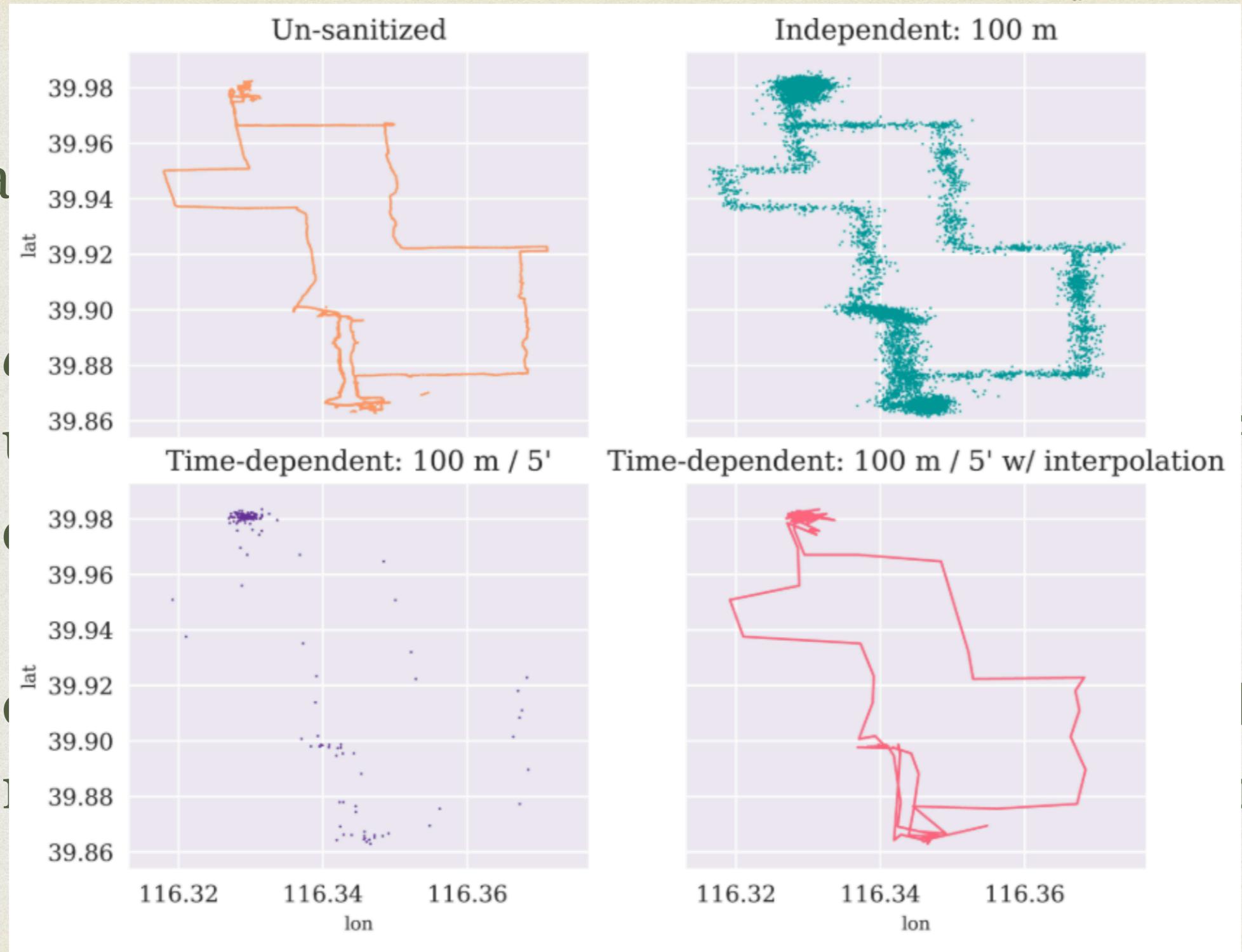
- Garantie dépend fortement du facteur k : indistingabilité = $1/k$
 - quel k choisir pour ne pas trop perturber l'utilité (souvent k=2 pour des trajectoires) ?
- **Grande surface d'attaque**
 - Protection contre **l'unicité** des profils mais c'est tout !
 - Et si les k individus se rendent tous à l'hôpital, que puis-je inférer ?
 - Restent possibles : attaques **d'appartenance**, de **co-localisation** et **divulgation des lieux visités**, etc.
 - Sensible à la sortie de nouveaux jeux de données (croisement, **chainage**)

MAIS ALORS ?

- La DP à la rescouisse !
- ϵ -géo-indistingabilité : un adv. ne peut savoir (avec une confiance l) si une localisation a été modifiée où non dans un rayon r $\epsilon = l/r$
- efficace pour protéger des points uniques (POI)
- malheureusement pas pour une trajectoire
 - trop de corrélation entre des positions en mouvement
 - idée : échantillonner ?

MAIS ALORS ?

- La

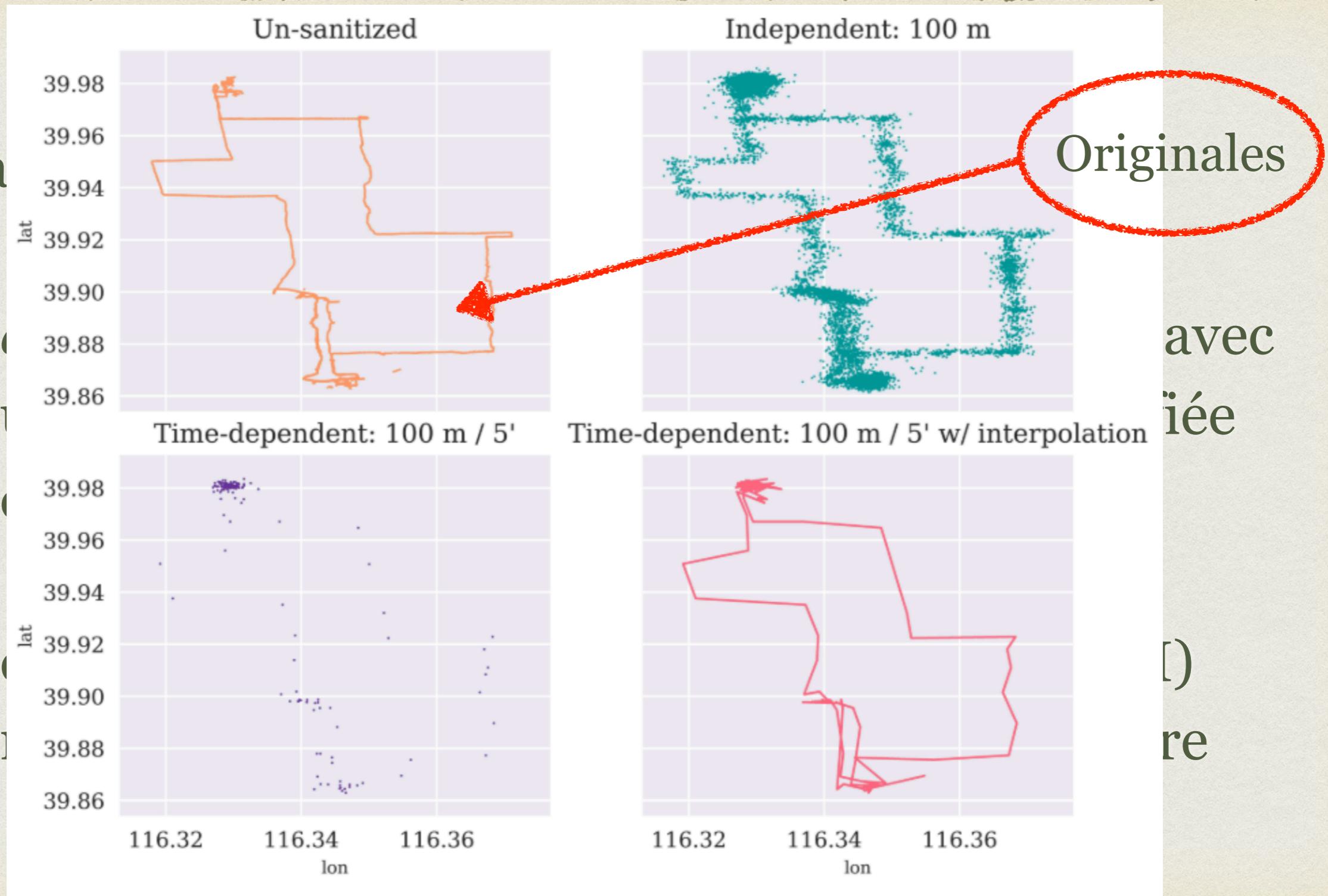


avec
iée

D
re

MAIS ALORS ?

- La

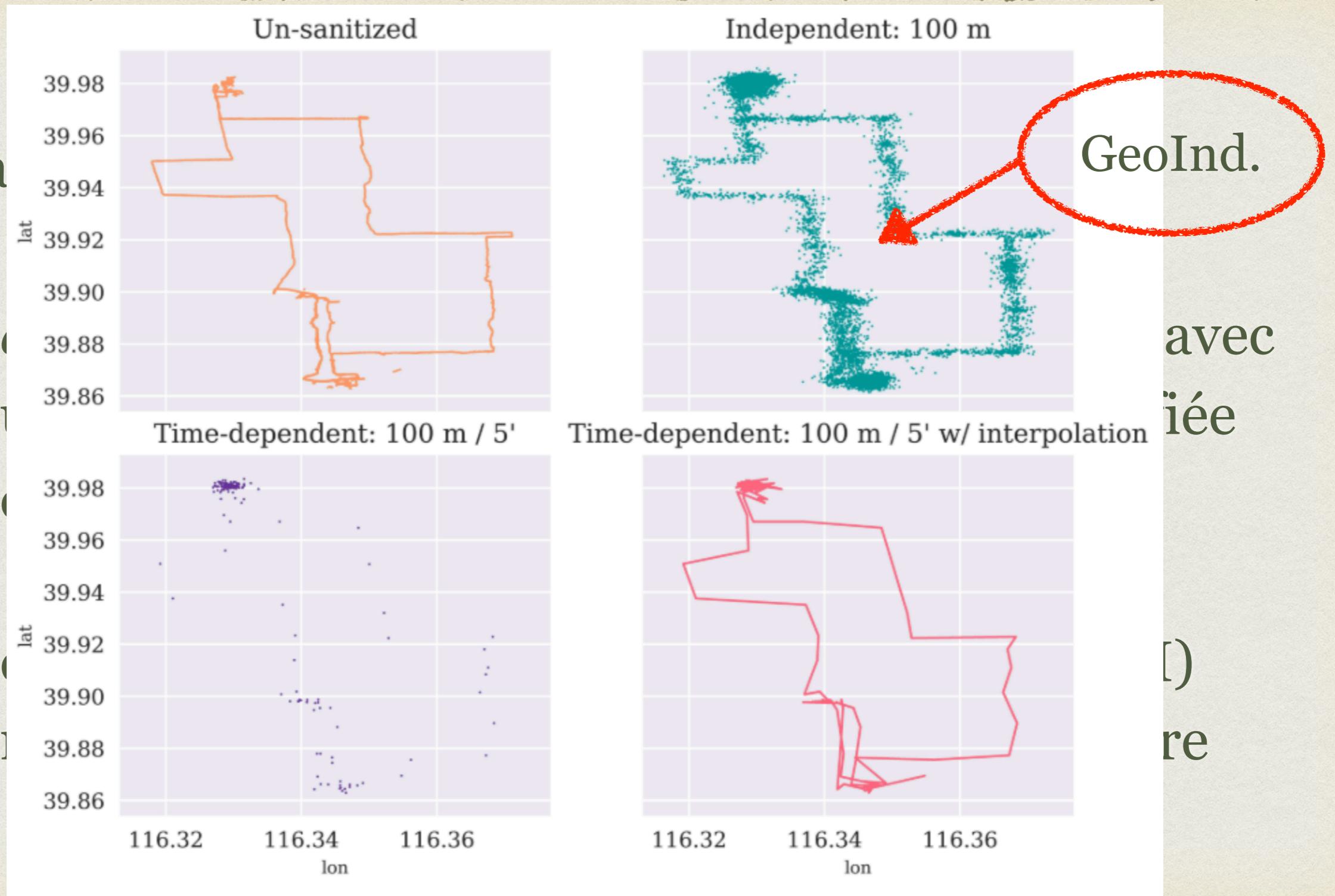


avec
iée

D
re

MAIS ALORS ?

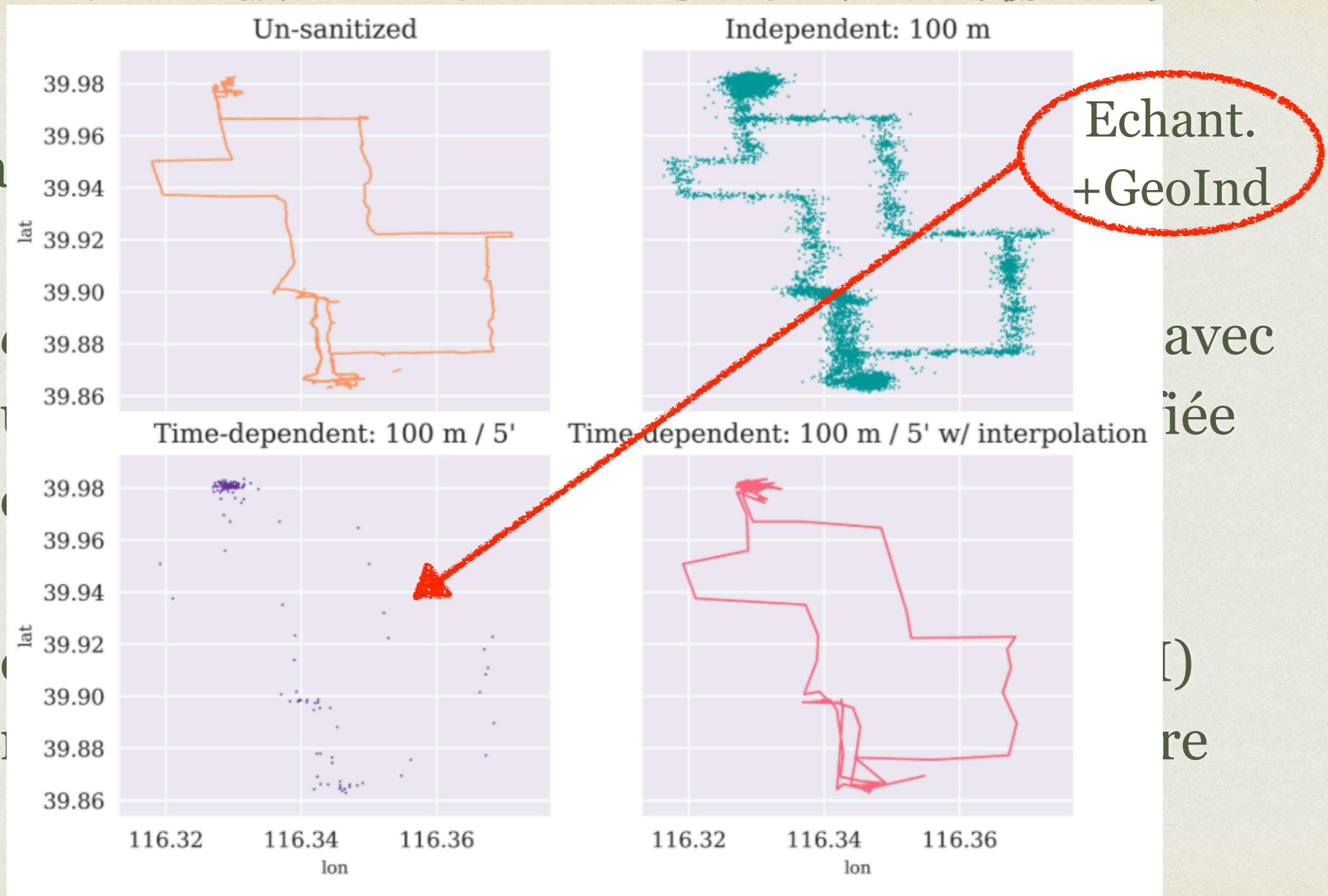
- La



avec
iée
D
re

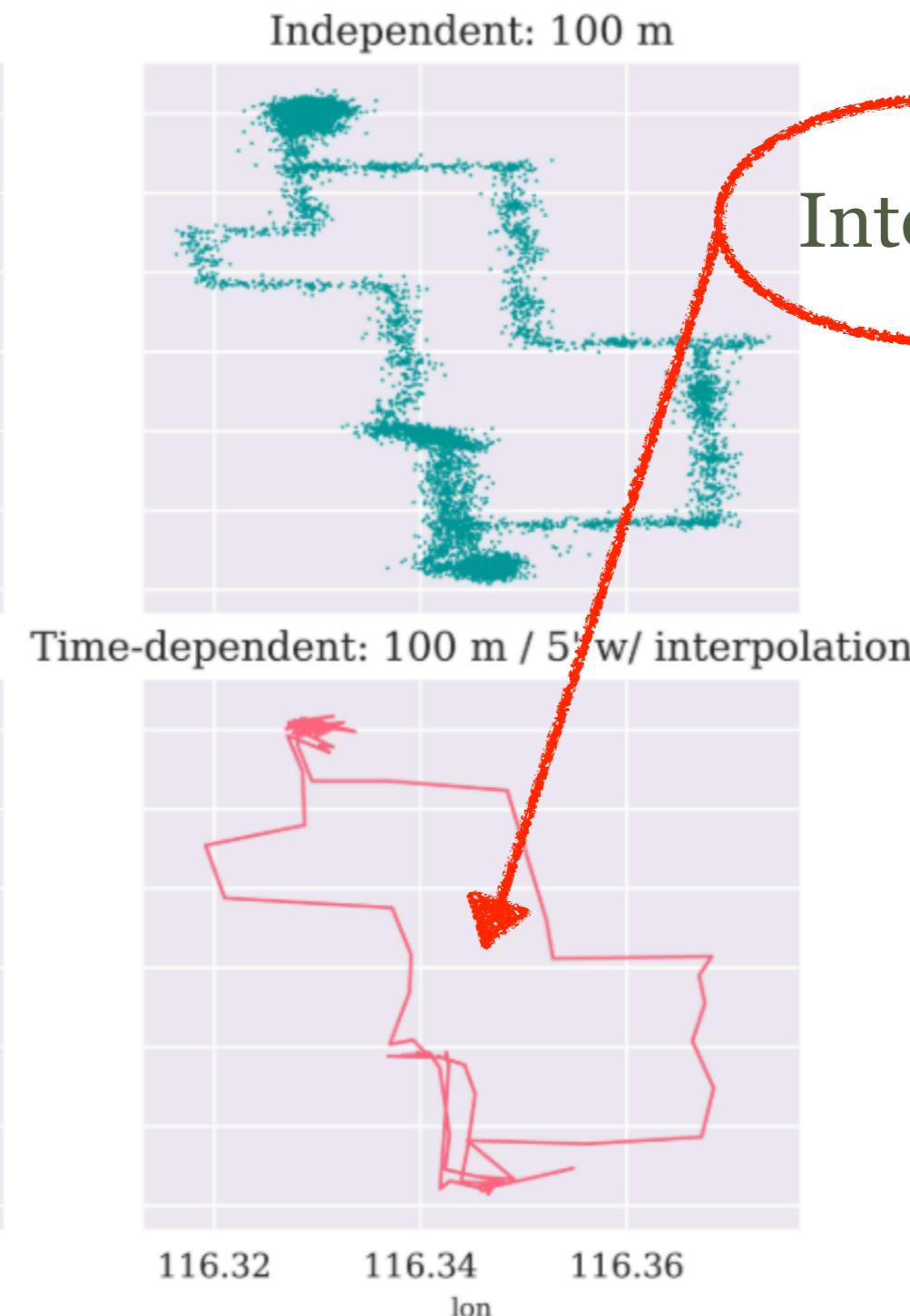
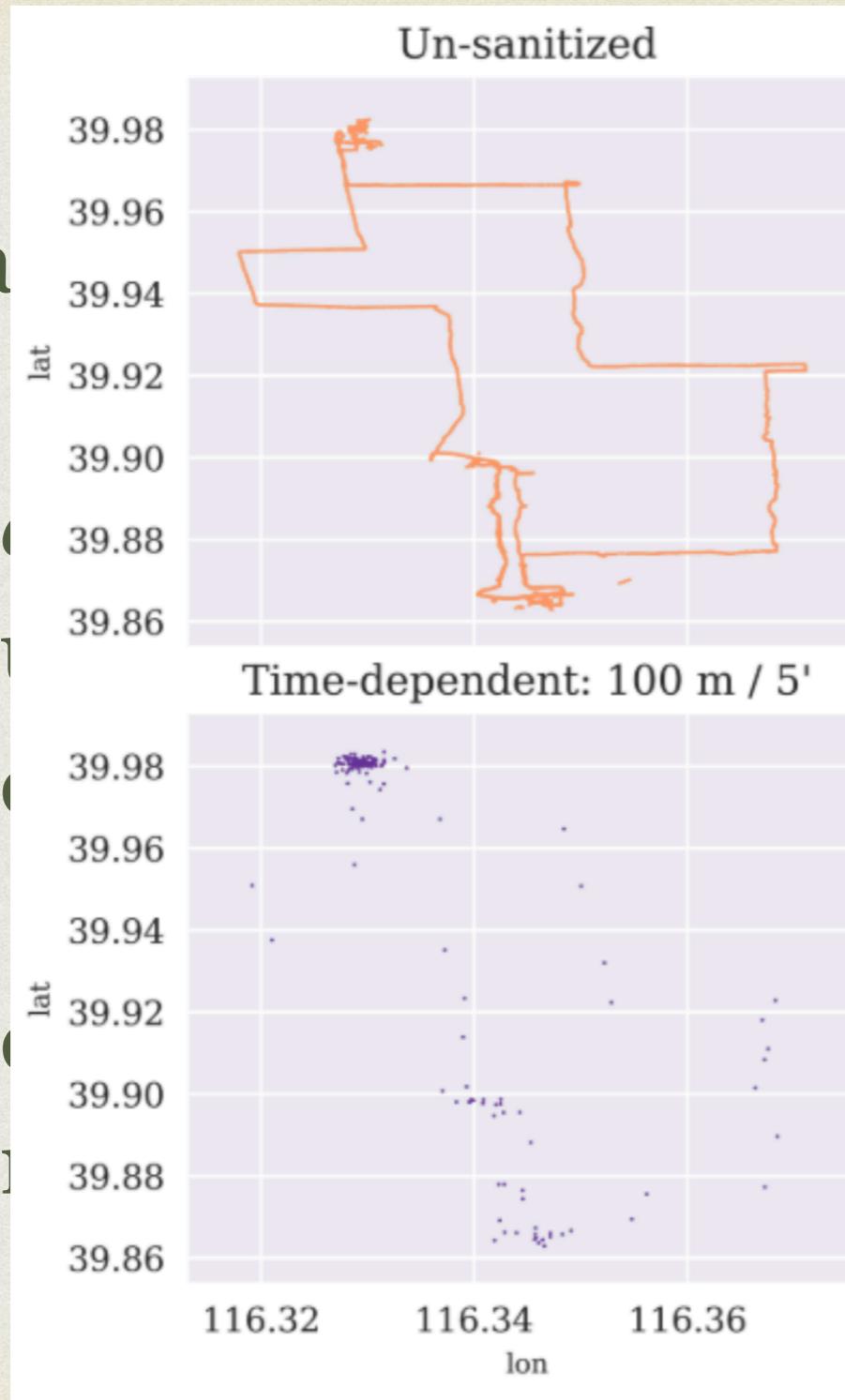
MAIS ALORS ?

- La
-
-
-
-
-
-
-
-
-



MAIS ALORS ?

- La



Interpol.

avec
iée

D
re

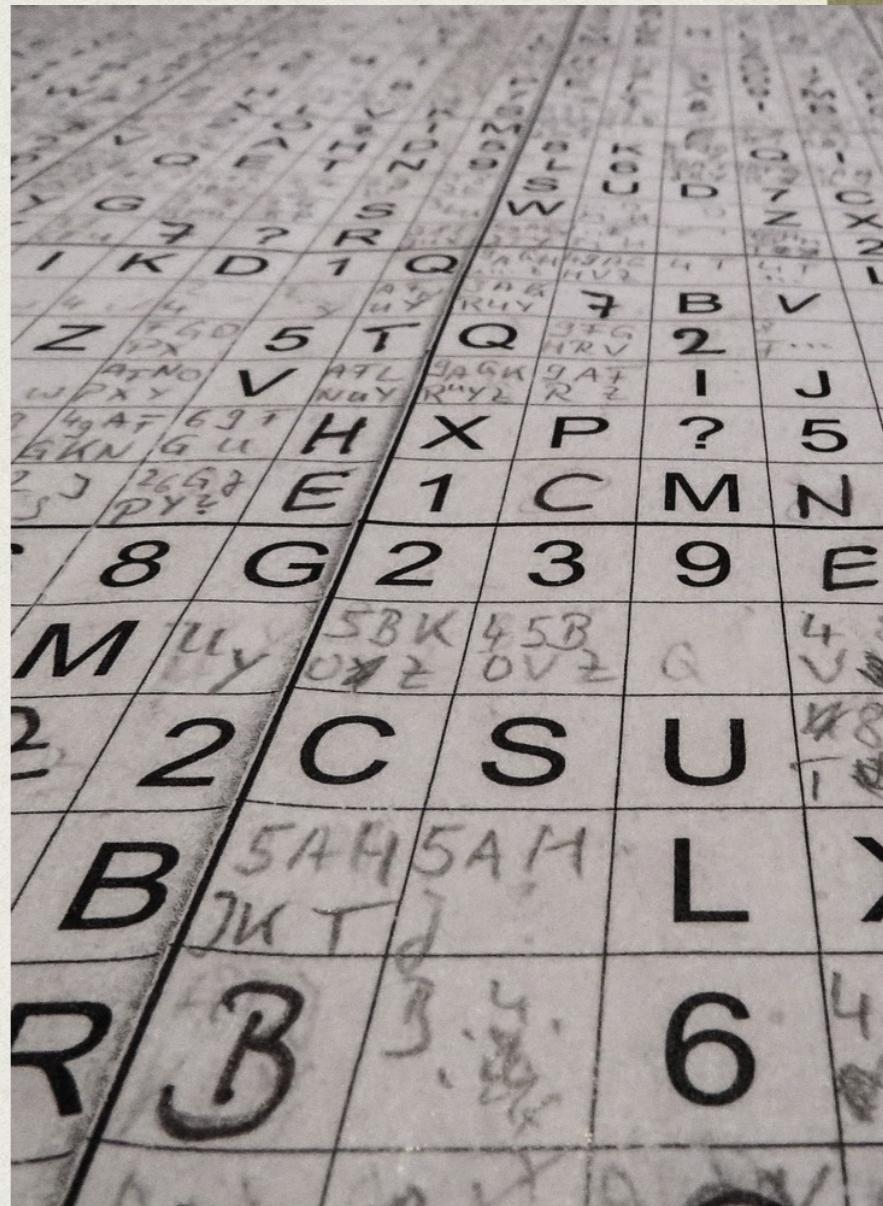
POUR CONCLURE

- Les données de géolocalisation sont **riches en utilité** et en **risques** de VP
- **Attaques faciles** car très identifiantes, corrélées, nombreuses, ubiquitaires, etc.
- **Protection difficile** car ... même raisons
- Il faut éviter de les semer à tout vent !

ANALYSE DE RISQUES

LA DIFFICULTÉ DE LA SÉCURITÉ INFORMATIQUE

- **Infaillibilité**
pour de nombreuses attaques, l'attaquant n'a besoin que de réussir **1 seule fois**
- **Ubiquité**
Postes: actualiser et migrer SEs et apps
Infrastructure réseau: actualiser (matériel, firmware, SEs, configurations) et surveiller (débits, flux)
Utilisateurs: actualiser (rôles, départs/arrivées, droits), sensibiliser, surveiller (mdp, accès)
Logiciels métiers, logiciels de sécurité, etc.
- **Tout savoir**
Faire de la veille sur tout ces points
Avoir tout prévu (ou plutôt que personne ne pense à quelque-chose que l'on n'a pas prévu)
- **Energie infinie**
Les attaquants ont une portée planétaire (pas d'horaire)
... sont nombreux
... n'ont rien d'autre à faire
... sont teigneux et passionnés



PRINCIPE DE BASE

- L'attaquant gagnera
 - A. Jamais
 - B. Lorsque je serais mort
 - C. Toujours
 - D. De la prison

PRINCIPE DE BASE

- L'attaquant gagnera
 - A. Jamais
 - B. Lorsque je serais mort
 - C. Toujours**
 - D. De la prison

PRINCIPE DE BASE (2)

- Vu qu'on va perdre, autant
 - A. Ne pas se défendre
 - B. S'y préparer
 - C. Changer de job

PRINCIPE DE BASE (2)

- Vu qu'on va perdre, autant
 - A. Ne pas se défendre
 - B. S'y préparer
 - C. Changer de job

PRINCIPE DE BASE (2)

- Vu qu'on va perdre, autant
 - A. Ne pas se défendre
 - B. S'y préparer**
 - C. Changer de job

SE PRÉPARER AU PIRE

- Si la dernière barrière tombe ?
 - Puis-je revenir en arrière (sauvegardes) ?
 - Puis-je tout couper ?
 - Qui dois-je prévenir ?
 - Quel protocole pour revenir à une situation normale ?
- Et dans ce cas
 - Quelle est l'**étendue des dégâts** ?
 - Combien de temps avant **recouvrement** ?
 - Comment couvrir ses **pertes** ?



ANALYSE DE RISQUE (1)

- L'analyse de risque, des risque, du risque, l'appréciation des risques
- c'est **préparer** son organisation, son entreprise, son système d'information **à une attaque**
- **identifier les actifs, les menaces et vulnérabilités**
- **évaluer les risques**
- **identifier des solutions** et les prioriser
- **auditer et recommencer**

ANALYSE DE RISQUE (2)

- identifier des solutions
 - définir des **politiques de sécurité** (acteurs, rôles, services, droits)
 - mettre en place une **organisation de la sécurité** (responsables, protocoles)
 - définir des **plans de recouvrement** (comment on fait quand le SI est ou est en train de tomber?)
 - prévoir une **réponse à incident** (les attaquants sont-ils encore là? de quelles bases saines on dispose? que fait-on si on trouve qui a attaqué? etc.)
 - **former** les usagers

ANALYSE DE RISQUE (2)

- identifier des solutions
 - définir des **politiques de sécurité** (acteurs, rôles, services, droits)
 - mettre en place une **organisation de la sécurité** (responsables, protocoles)
 - définir des **plans de recouvrement** (comment on fait quand le SI est ou est en train de tomber?)
 - prévoir une **réponse à incident** (les attaquants sont-ils encore là? de quelles bases saines on dispose? que fait-on si on trouve qui a attaqué? etc.)
 - **former les usagers**

Sans ça, ça peut prendre des mois !!!

ANALYSE DE RISQUE (3)

- Ce n'est pas facile, ça peut paraître ennuyeux, mais c'est **essentiel** dans une entreprise, moyenne ou grande
- On peut facilement **passer à côté** de quelque-chose
- Alors il y a des **méthodes** pour nous guider, beaucoup de méthodes
 - CRAMM, EBIOS, Mehari, TIK, Octave, etc.
- Et des **normes**, beaucoup de normes...
 - ISO 27000 et **27001**, ISO 13335, ISO 15408, ISO 17799, ISO 21287
- Mais on s'en dans les activités de la semaine vous allez regarder **EBIOS-RM** (efficace, pratique, gratuite, adaptable) et vous aurez une bonne idée de ce à quoi peuvent ressembler les autres.