Lecture Notes on

Pattern Recognition

Session 07: Data Science – The Risk of Privacy Compromise

Gang Li
School of Information Technology
Deakin University, VIC 3125, Australia

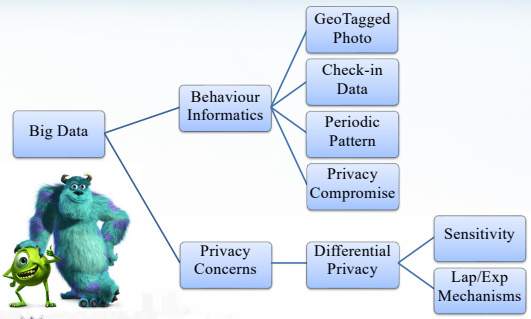
0

Unit Learning Outcomes

- **ULO1**:
  - Develop knowledge of and discuss new and *emerging fields* in data science.
    - Why there is the risk of privacy compromise
    - What are the current method to preserve the privacy?
    - How to manipulate textual data?
- **ULO2**:
  - Describe advanced constituents and underlying *theoretical foundation* of data science.
    - The principle of differential privacy

1

Road map



2

Research Themes @ TULIP Lab

(Team for Universal Learning and Intelligent Processing)

- Research Themes
  1. Behavior Informatics
     - *Periodic Behavior Mining*
     - *Behavior Prediction*
  2. Information Abuse Prevention
     - *Privacy Preserving Data Mining*
     - *Information Releasing Compliance Checking*
  3. Business Intelligence Applications
     - Recommender System
     - Tourism/Hospitality Management

3

Behavior Informatics

- Geotagged Photo
- Check-in Data
- What can be discovered?

4

Behavior Informatics

- People share news, interests and ideas in OSNs,
  - **though** these platforms also spread email malware, rumours, gossips and malicious links, and also leak our privacy.

5

Tourist Movement Analysis

- **Tourism Managers** need to obtain a comprehensive understanding about tourist behaviour:
  - *Where and when visited?*
  - *What are participated activities and events?*
  - *What are tourist preferences and perceptions toward tourism products and service?*
  - ……

6

Tourist Movement Analysis

- **Existing Approaches in Travel Behavior:**
  - Survey and opinion polls are popular methods.
  - Time consuming and limited in the number of responses and scale of surveyed areas.

SOCIAL MEDIA ANALYTICS

- **Challenges:**
  - *How to capture comprehensive information about tourist travel behavior at large scales?*
  - *How to extract meaningful insights about tourist travel behavior?*

7

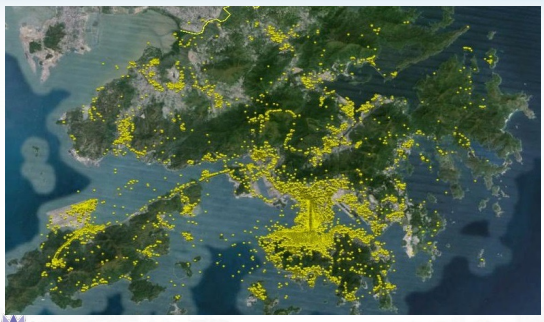
Geotagged Photos

- Many photo-capturing devices now have built-in global positioning systems (GPS) technology

- **Geotagged photos** are shared on social website
  - Flickr (*www.flickr.com*)
  - Panoramio (*www.panoramio.com*)
  - **29,443 photos** collected from **2,100 HK inbound tourists**

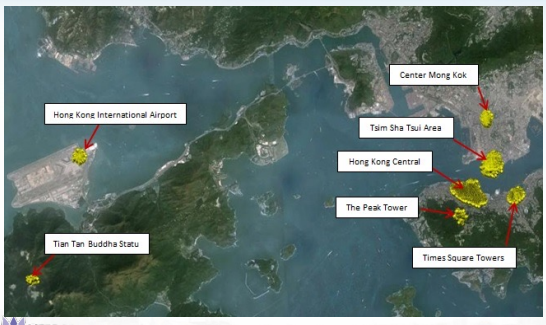
8

Geotagged Photos Visualization



9

Geotagged Photos Visualization



10

Hot Spots

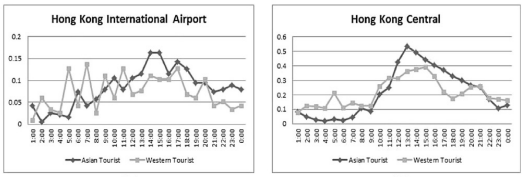
Popularity of Areas of Interest.

Group	Area of Interest	Percentage (%)	Popularity Rank
Asian Tourist	Hong Kong Central	40.35	1
	Tsim Sha Tsui Area	38.80	2
	Times Square Towers	20.08	3
	Hong Kong International Airport	18.34	4
	The Peak Tower	14.19	5
	Center Mong Kok	10.52	6
Western Tourist	Hong Kong Central	47.92	1
	Tsim Sha Tsui Area	44.64	2
	The Peak Tower	19.74	3
	Center Mong Kok.	15.14	4
	Times Square Towers	12.22	5
	Hong Kong International Airport	10.99	6
	Tian Tan Bubbha Statue	10.43	7

11

Temporal Analysis

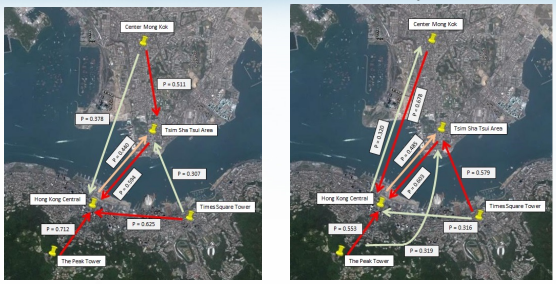
- Tourist Present based on time stamp of the photos



(A) (B)

12

Tourist Movement Analysis

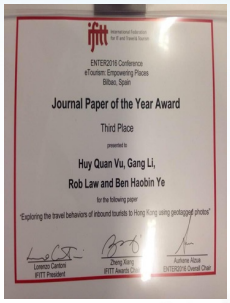


(A) Asian Tourist (B) Western Tourist

Tourist Traffic Flow in Hong Kong Metropolitan Area.

13

Tourist Movement Analysis

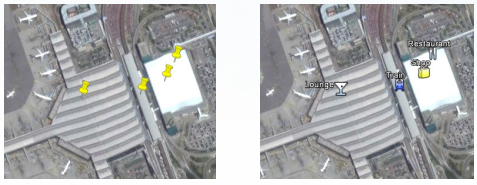


Huy Quan Vu, Gang Li, Rob Law, Ben Haobin Yip. *Exploring the travel behaviors of inbound tourists to Hong Kong using Geotagged photos*. **Tourism Management**.

14

What is more?

- Geotagged Photos cannot provide detailed contextual information on tourists' activities for further analysis



(a) Without Activity Information (b) With Activity Information

15

Venue Check-ins

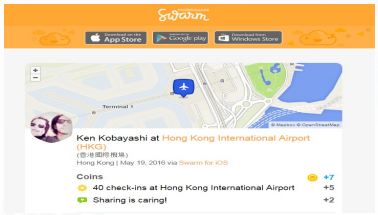
- Location-aware mobile social applications, including
  - Foursquare (www.foursquare.com)
  - Ubersocial (www.ubersocial.com)
  - Yelp (www.yelp.com)

- Available on mobile devices
  - Allow users to explicitly share their current location in the form of venue check-ins,
    - With metadata such as *venue name*, *categories*, and *subcategories*.
  - Allows for **inferring tourist activities** (*dinning, shopping, sightseeing, entertainment*, etc.)

16

Venue Check-ins

- One Example
  - https://www.swarmapp.com/c/8tfAWSjlQjU



17

Foursquare Venues

Activity category (Label)	Example of Venue Type
Art & Entertainment (At)	Arcade, Art Gallery, Casino, Circus, Concert Hall, Exhibit, Historic Site, Movie Theater, Museum, Stadium, Theme Park, Zoo
College & University (Co)	College Academic Building, College Bookstore, College Library, College Lab, Student Center
Event (Ev)	Christmas Market, Conference, Convention, Festival, Parade
Food (Fo)	American Restaurant, Asian Restaurant, Italian Restaurant, Seafood Restaurant, Fast Food Restaurant, Burger Joint, Food, Court, Coffee Shop, Dessert Shop
Nightlife Spot (Ni)	Bar, Lounge, Night Market, Nightclub
Outdoors & Recreation (Ou)	Athletics & Sports, Bay, Beach, Bike Trail, Botanical Garden, Bridge, Campground, Harbor /Marina
Professional & Other Places (Pr)	Animal Shelter, Auditorium, Ballroom, Building, Community, Center, Convention Center, Cultural Center, Factory, Spiritual Center
Residence (Re)	Assisted Living, Home, Housing Development, Residential Building, Trailer Park
Shop & Service (Sh)	ATM, Antique Shop, Business Service, Flower Shop, Food & Drink Shop, Gaming Café
Travel & Transport (Tr)	Airport, Boat or Ferry, Bus Station, Cable Car, Cruise, Hotel, Metro Station, Pier, Taxi Stand

https://developer.foursquare.com/categorytree

18

Check-in Data

- Check-in Record of a Tourist during a trip in Hong Kong

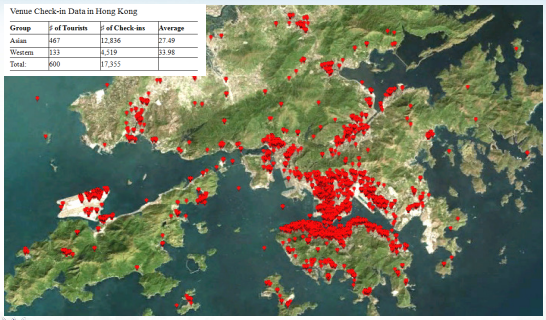
ID	Date	Time	Venue Name	Venue Type	Category	latitude/longitude
C1	4-Jun-16	18:47	Hong Kong International Airport	Airport	Tr	22.3153 / 113.9348
C2	4-Jun-16	22:35	Tsim Sha Tsui	Neighborhood	Ou	22.3001 / 114.1726
C3	4-Jun-16	22:41	KFC	Fried Chicken Joint	Fo	22.2989 / 114.1728
C4	5-Jun-16	17:17	Ngong Ping	Neighborhood	Ou	22.2550 / 113.9069
C5	5-Jun-16	17:18	Ngong Ping 360 Station	Cable Car	Tr	22.2563 / 113.9014
C6	5-Jun-16	17:18	Walking with Buddha	General Entertainment	At	22.2564 / 113.9031
C7	5-Jun-16	19:26	Tsing Chau Tsai	City	Ou	22.3090 / 114.0255
C8	5-Jun-16	21:55	The Spaghetti House	Italian Restaurant	Fo	22.2962 / 114.1714
C9	6-Jun-16	11:37	Ocean Park Hong Kong	Theme Park	At	22.2479 / 114.1743
C10	6-Jun-16	11:38	Giant Panda Adventure	Zoo	At	22.2453 / 114.1754
C11	6-Jun-16	11:39	Panda Village	Zoo	At	22.2461 / 114.1762
C12	6-Jun-16	19:47	Spoon by Alain Ducasse	French Restaurant	Fo	22.2932 / 114.1741
C13	6-Jun-16	21:18	Sheraton Hong Kong Hotel	Hotel	Tr	22.2953 / 114.1726
C14	6-Jun-16	22:18	McDonald	Fast Food Restaurant	Fo	22.2964 / 114.1711
C15	7-Jun-16	12:46	MTR Tung Chung Station	Metro Station	Tr	22.2892 / 113.9413
C16	7-Jun-16	14:49	Leonidas	Chocolate Shop	Fo	22.2891 / 113.9407
C17	7-Jun-16	19:28	Cross-Harbour Tunnel	Tunnel	Tr	22.2935 / 114.1817
C18	7-Jun-16	20:36	The Peak Galleria	Shopping Mall	Sh	22.2703 / 114.1500
C19	7-Jun-16	20:37	Victoria Peak	Mountain	Ou	22.2708 / 114.1496
C20	8-Jun-16	9:01	Hong Kong International Airport	Airport	Tr	22.3153 / 113.9348

19

Check-in Data

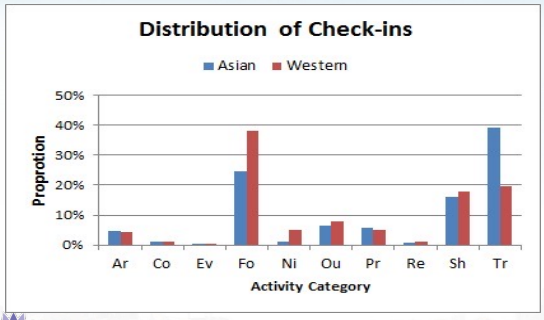
Venue Check-in Data in Hong Kong

Group	# of Tourists	# of Check-ins	Average
Asian	467	12,836	27.49
Western	133	4,519	33.98
Total:	600	17,355	



20

Activity Categories Distribution



21

Activity Preference Analysis

Activity Preferences of *Asian* and *Western* tourists

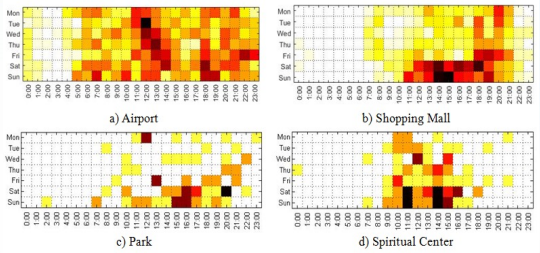
Venue Type	Proportion (%) Asian	Western	Difference	Z-test z-score	p-value*
Arts & Entertainment					
Theme Park	27.74	8.27	19.47	4.655	0.000
Food					
Hong Kong Restaurant	19.14	9.77	9.37	2.514	0.012
Steakhouse	2.58	9.02	6.44	−3.350	0.011
Nightlife Spot					
Bar	4.73	14.29	9.55	−3.860	0.000
Lounge	1.29	8.27	6.98	−4.283	0.000
Pub	0.22	6.77	6.55	−5.207	0.000
Hotel Bar	3.23	8.27	5.04	−2.527	0.011
Cocktail Bar	1.51	6.02	4.51	−2.943	0.003
Outdoors & Recreation					
Neighborhood	30.32	18.80	11.53	2.591	0.010
City	11.40	20.30	8.90	−2.679	0.007
Shop & Service					
Shopping Mall	40.22	27.07	13.15	2.731	0.006
Travel & Transport					
Metro Station	14.84	3.76	11.08	3.408	0.001
Train Station	12.90	4.51	8.39	2.710	0.007
Bus Stop	5.16	0.00	5.16	2.668	0.008

*Significant at $p \leq 0.05$

22

Temporal Analysis

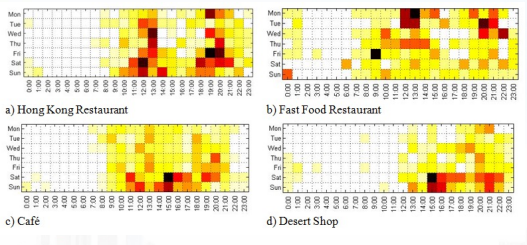
- Tourism Spots



23

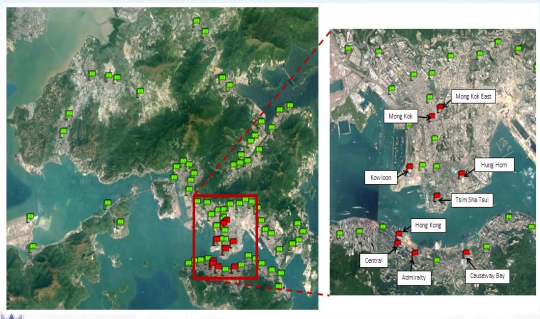
Temporal Analysis

- Dinning Behavior



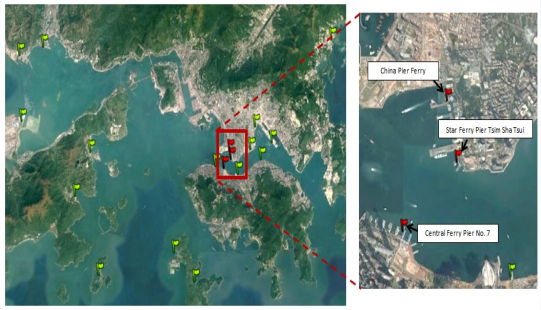
24

Train Station Visits



25

Ferry Pier Visits



26

Tourists' Behavior Mining

Huy Quan Vu, Gang Li, Rob Law, Yanchun Zhang. Travel Diaries Analysis by Sequential Rule Mining. **Journal of Travel Research**, 2017, 57(3): 399-413.

27

Periodic Behavior Mining

- Observed Check-in Data is usually a mixed events from different periodic behaviors
  - What are regular behavior patterns?
  - What are their periods for each?
  - Predict the Behavior on a particular day

28

Periodic Behavior Mining

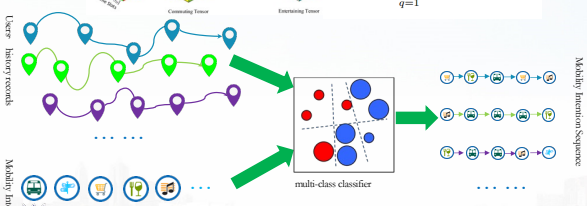
- Observed Check-in Data is usually a mixed events from different periodic behaviors
  - What are Periodic?
  - What is the period?
  - Predict the Behavior on a particular day

29

Periodic Behavior Mining
Mobility Intentions

- CP Decomposition

$$y_{r_i,t_j,d_k} = \frac{Count(r_i,t_j,d_k)}{\sum_{q=1}^{L} Count(r_q,t_j,d_k)}$$



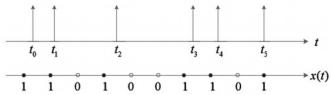
30

Periodic Behavior Mining
Periodicity Detection

Definition 1 (Human Periodic Behavior). *Suppose $T_0 > 1$ and $0 \leqslant t_0 < T_0$, for any $0 \leqslant t^* < T_0$*

$$\mathrm{I}(t^*) = \begin{cases} 1, t^* = t_0 \\ 0, \text{otherwise} \end{cases}. \quad (1)$$

If there is one and only one timestamp $t' \in [t_0-\delta+kT_0, t_0+\delta+kT_0]$ of X which satisfies $\mathrm{I}(t') = \mathrm{I}(t_0)$ for $k = 0, 1, \ldots,$ $\mod(n-1, T_0)$, the binary sequence X is a periodic behavior binary sequence *with the period T_0.*

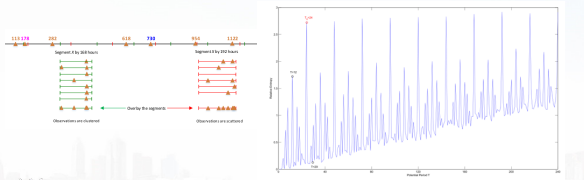


31

Periodic Behavior Mining
Periodicity Detection

Lemma 1. *If a binary sequence X is periodically generated according to a categorical distribution $\boldsymbol{\mu}_0'$ for some period T_0, then for any $T \geqslant 2, T \in \mathbb{N}$, we have*

$$\lim_{n\to\infty} \mathrm{KL}(T_0) \geqslant \lim_{n\to\infty} \mathrm{KL}(T) \quad (5)$$



32

Periodic Behavior Mining
Applications

- Applications of Periodic Behavior Mining
  - What is the schedule of a person on a particular day/time?
  - Where to find the person on a particular day/time?
    - Police applications
    - Scheduled "Encountering" for match making
  - Timely Recommendation Systems
    - Now it is the time for you to stock rice, cooking oil, or ice cream!

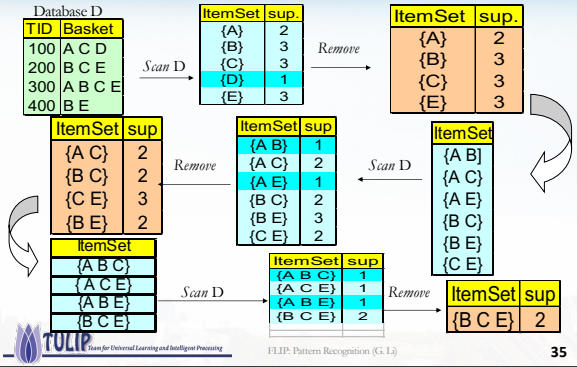
33

Privacy Breach

- Privacy Breach in Data Release/Sharing:
  - Adversary with background information, may **re-identify the user** or **confirm the relationship** between users from the **aggregated information** of the dataset.
    - Adversary observes the **aggregated information** of the dataset, removing a particular user will change the statistical information.

34

Apriori Algorithm: Example



35

Privacy Breach Example (1)

TABLE 5. Privacy breach of international visitors

ID	User(Gender)	Location of Origin	Venue	Date	Time
R_1	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	Rendezvous Hotel Singapore	31-Dec-2015	10:24
R_2	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	Plaza Singapura	31-Dec-2016	17:22
R_3	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	Gardens by the Bay	31-Dec-2016	20:58
R_4	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	The Cathay Cineplex	1-Jan-2017	14:15
R_5	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	Sentosa Island	1-Jan-2017	16:01
R_6	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	Siloso Beach	1-Jan-2017	17:10
R_7	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	FashionTV Singapore Night Club	2-Jan-2017	02:14
R_8	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	MA Deen Biasa Restaurant	2-Jan-2017	04:27
R_9	U_1(M)-U_2(F)	Kuala Lumpur, Malaysia	Merlion Park	2-Jan-2017	18:09

36

Privacy Breach Example (2)

TABLE 6. Privacy breach of Singapore residents traveling overseas.

ID	User(Gender)	Visited Destination	Venue	Date	Time
L_1	U_5(M)-U_6(F)	Shanghai, China	UNCO Lounge	25-May-2015	20:17
L_2	U_5(M)-U_6(F)	Shanghai, China	T8 Restaurant and Bar	26-May-2015	17:35
L_3	U_5(M)-U_6(F)	Cannes, France	Villa Mystique Resort	25-Jun-2015	11:03
L_4	U_5(M)-U_6(F)	Paris, France	Dersou Restaurant	27-Jun-2015	19:58
L_5	U_5(M)-U_6(F)	Paris, France	Ladure Pastry Shop	28-Jun-2015	14:48
L_6	U_5(M)-U_6(F)	London, United Kingdom	L'ETO Caff	10-Oct-2015	11:01
L_7	U_5(M)-U_6(F)	Hong Kong	The Ocean Club Bar	31-Oct-2015	18:47
L_8	U_5(M)-U_6(F)	Hanoi, Vietnam	HOME Hanoi Restaurant	01-Jan-2016	19:04
L_9	U_5(M)-U_6(F)	Ho Chi Minh, Vietnam	MGallery Hotel des Art	30-Jun-2016	19:54
L_{10}	U_5(M)-U_6(F)	Ho Chi Minh, Vietnam	L'Usine: Cafe	01-Jul-2016	10:55
L_{11}	U_5(M)-U_6(F)	Ho Chi Minh, Vietnam	Social Club @ Hotel Des Arts	01-Jul-2016	17:04

37

Privacy Breach Example (3)

TABLE 7. Privacy breach of local resident in Singapore.

ID	User(Gender)	Venue	Date	Time
S_1	U_7(M)-U_8(F)	Club Myst	01-May-2017	01:56
S_2	U_7(M)-U_8(F)	Strker Signature Bar	10-May-2017	21:16
S_3	U_7(M)-U_8(F)	Club Hollywood	13-May-2017	00:20
S_4	U_7(M)-U_8(F)	Oppa Korean Grill Restaurant	16-May-2017	19:17
S_5	U_7(M)-U_8(F)	MANEKINEKO Karaoke Bar	19-May-2017	22:09
S_6	U_7(M)-U_8(F)	Hotel G Singapore	10-Jun-2017	11:24
S_7	U_7(M)-U_8(F)	Golden Village Multiplex	08-Jul-2017	21:24
S_8	U_7(M)-U_8(F)	The Platinum Movie Suites	12-Aug-2017	14:35
S_9	U_7(M)-U_8(F)	Joo Bar	12-Aug-2017	19:46

38

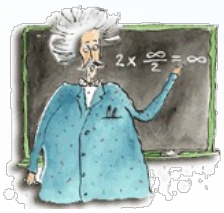
Privacy Breach Example (4)

TABLE 8. Joint check-in record indicating sensitive contrast relationship.

ID	User(Gender)	Venue	Date	Time
C_1	U_9(M)-U_{10}(F)	Zouk Night Club	11-Sep-2015	23:31
C_2	U_9(M)-U_{11}(F)	Zouk Night Club	18-Nov-2015	23:50
C_3	U_9(M)-U_{11}(F)	Club Luxi	17-Jan-2016	00:30
C_4	U_9(M)-U_{11}(F)	Club Hollywood	06-Feb-2016	04:34
C_5	U_9(M)-U_{10}(F)	Wave House Sentosa	12-Mar-2016	22:43
C_6	U_9(M)-U_{10}(F)	Zouk Night Club	02-Jul-2016	00:25
C_7	U_9(M)-U_{10}(F)	Zouk Night Club	07-Aug-2016	00:39

39

Concerns on Data Privacy



- Privacy Model
- Differential Privacy

40

Special Issues on Privacy

- IEEE Spectrum, Aug. 2014
  - On the Internet, nobody knows you are a dog (1993).
  - Interested parties not only know you are a dog, but also know the colour of your fur (2014)

41

Special Issues on Privacy

- **Communication of ACM** Sept. 2014
  - Federal law governing student privacy and the release of student records suggests that anonymizing student data can hardly protects student privacy.


practice

Privacy, Anonymity, and Big Data in the Social Sciences

42

Special Issues on Privacy

- **Science**, Jan. 2015
  - Data pour out of us and our devices every second of every day, and people no longer control their personal privacy.

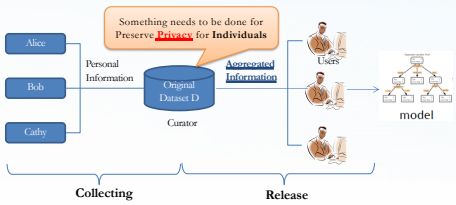
43

Information Abuse Prevention

- **Information Abuse**
  - The compromise of information for which the data stakeholders are not willing to disclose.
  - It depends on
    - the nature of the information,
    - the involved internal or external users,
    - and the ways in which the organization grants the access to or releases the information.

44

Background



Data are collected in:
- Medical, Bank, Social Network……

Social benefits :
- better services, Finding correlations, Publishing official statistics, Data Mining……

45

Who is an adversary?

- Every user is potentially an adversary
  - After data is released, we cannot prevent any user from performing any type of analysis on the released data
  - Worst case scenario
    - Must account for disclosure risk from all types of analyses

46

RR: One Early Trick in Social Science

- Response to embarrassing questions
  - How many percentage of researchers are using pirate software?
  - ***Are you using Pirate Software in research?***
    - ***Yes?***
    - ***No?***

- Participants are advised to response as below
  - Flip a coin
    - If ***tail***, then response the truth
    - If ***head***, flip another coin
      - If ***head***, response **Yes**
      - If ***tail***, response **No**

47

RR: One Early Trick in Social Science

- Response to embarrassing questions
  - How many percentage of researchers are using pirate software?
  - ***Are you using Pirate Software in research?***
    - ***Yes?***
    - ***No?***
- Here privacy comes from ***a plausible deniability*** of any outcome
- Accuracy comes from the understanding of the mechanism
  - expected #Yes is
    - ¼ participants who are not Yes +
    - ¾ participants who are Yes
    - P'=¼(1-p)+¾ p = ¼+p/2

48

What to promise?

- Respondent will feel safe submitting his data if

"If I knew the chance that the privatized **aggregated information** (constructed model or query results) S was **nearly the same**, whether or not I submitted my information"

49

What to promise?

- Respondent will feel safe submitting his data if

"If I knew the chance that the privatized **aggregated information** (constructed model or query results) S was **nearly the same**, whether or not I submitted my information"

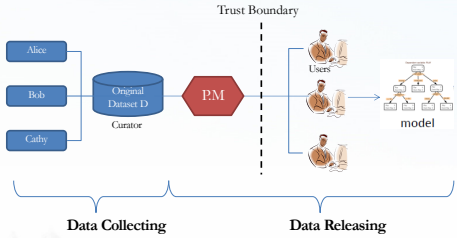
It bounds the ability to infer from any outcome S, whether the input data was D or D'.

From an arbitrary prior P(D) and P(D'), we see that

$$\frac{p(D|S)}{p(D'|S)} = \frac{p(D)}{p(D')} \times \frac{p(S|D)}{p(S|D')}$$

50

Privacy Model

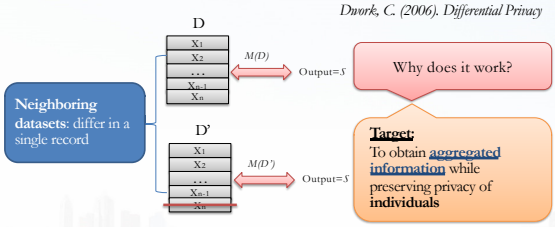


51

Differential Privacy

- An individual is **in** or **out** of the database should make **little difference** of the analytical output

Dwork, C. (2006). Differential Privacy



52

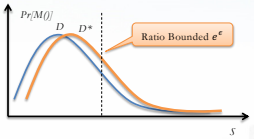
Differential Privacy

- Definition:
  - a mechanism ***M*** is *ϵ-differential privacy* if for all pairs of neighboring datasets ***D*** and ***D'***, and for all possible output ***S***, satisfy with:

ϵ is Privacy Budget

$$e^{-\epsilon} \leq \frac{\Pr[M(D) \in S]}{\Pr[M(D') \in S]} \leq e^{\epsilon}$$

DP-Mechanism



53

Privacy Budget

- ε controls the privacy guarantee level of mechanism.
  - A smaller ε represents a stronger privacy.
  - Normally, it is less than 1.

54

Sensitivity: Global Sensitivity

- The ***global sensitivity*** considers the maximal difference between query results on neighboring datasets
  - indicates how much the ***difference*** should be hidden in mechanisms
  - Only related to query

55

Sensitivity: Example

- Suppose we have a dataset D and two queries:
  f_1=Count(HIV), f_2=Average(Age).
- Let r represent the record.

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	50	Hepatitis
Lawyer	Male	35	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dance	Female	30	HIV

Count(HIV)	Average(Age)
f1(D)=4	f2(D)=34.3
f1(D-r1)=4	f2(D-r1)=34.1
f1(D-r2)=4	f2(D-r2)=31.6
f1(D-r3)=3	f2(D-r3)=34.1
f1(D-r4)=4	f2(D-r4)=35
f1(D-r5)=3	f2(D-r5)=35
f1(D-r6)=3	f2(D-r6)=35
f1(D-r7)=3	f2(D-r7)=35
Δf_{GS}=4-3=1	Δf_{GS}=34.3-31.6=2.7

56

Differential Privacy Mechanism

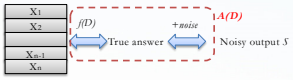
- ***Laplace*** Mechanism:
  - suitable for numeric output
    - How many people in this room have blue eyes?
- ***Exponential*** Mechanism:
  - suitable for non-numeric output
    - What is the most common eye color in this rooms?

Dwork, C., McSherry, F., Nissim, K., & Smith, A. (2006). Calibrating Noise to Sensitivity in Private Data Analysis. Theory of Cryptography , 265-284.
McSherry, F., & Talwar, K. (2007). Mechanism Design via Differential Privacy. (FOCS'07)

57

Laplace Mechanism

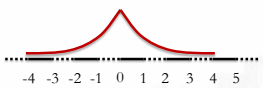
- Let *f(D)* be a numeric query on dataset *D*
  - How many people in this room have blue eyes?
  - The sensitivity of *f*: $\Delta f = max \parallel f(D) - f(D') \parallel_1$



  - A Laplace Mechanism M is ϵ-differential privacy:

$$M(D) = f(D) + Lap(\frac{\Delta f}{\epsilon})$$

True Answer | Noise

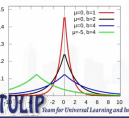


58

Laplace Example

Job	Sex	Age	Disease
Engineer	Male	35	Hepatitis
Engineer	Male	38	Hepatitis
Lawyer	Male	38	HIV
Writer	Female	30	Flu
Writer	Female	30	HIV
Dancer	Female	30	HIV
Dance	Female	30	HIV

$$Lap(b) = \frac{1}{2b}\exp(-\frac{|x|}{b})$$



- Query: How many people has HIV?
  - DP answer = True answer + Noise

$$M(D) = f(D) + Lap(\frac{\Delta f}{\epsilon})$$

  - Sensitivity is 1, because the answer is changed most at 1 if one user is deleted.
  - If we define Δf =1, the noise is sample from:

$$Lap(\frac{1}{\epsilon})$$

  - DP answer M(D):
    - 4 + 1 = 5 (higher probability)
    - 4 – 1 = 3 (higher probability)
    - 4 – 3 = 1 (lower probability)

59

Exponential Mechanism

- Exponential Mechanism is suitable for non-numeric output R
  - What is the most common eye color in this rooms?
    - i.e. R={Brown, Blue, Black, Green}

10%, 5%, 80%, 5%

  - Paired with a quality score q:
    - $q(D,r)$ represents how good an output r is for dataset D
- An exponential Mechanism A is ϵ-differential privacy if:

$$A(D,q) = \{return\ r\ with\ probability\ \propto \exp(\frac{\epsilon \cdot q(D,r)}{2\Delta q})$$

Sensitivity of q: $\Delta q = max \parallel q(D) - q(D^*) \parallel_1$

60

Exponential Example

- What is the most common eye color in this rooms?
  - i.e. R={Brown, Blue, Black, Green}

11.8%, 0.01%, 88%, 0.0001%

$$\Pr(r) \propto \exp(\frac{\epsilon \cdot q(D,r)}{2\Delta q})$$

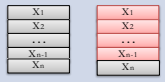
Impact of changing a single record

Option	Score	Sampling Probability		
		$\epsilon = 0$	$\epsilon = 0.1$	$\epsilon = 1$
Brown	23	0.25	0.34	0.12
Blue	9	0.25	0.16	10^{-4}
Black	27	0.25	0.40	0.88
Green	0	0.25	0.10	10^{-6}

61

Advantage of DP

	Traditional PM	Differential Privacy
Privacy level can be measured and compared	No	Can be measured by the privacy budget
The privacy guarantee can be proved theoretically	No	DP definition
Resist background attack	No	DP assumes that attackers get to know everyone's information except the one we will protect.



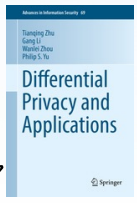
62

Challenge: Tradeoff P&U

- ***Privacy***
  - bounded by the privacy budget
- ***Utility***
  - diverse measurements according to different application requirements
    - Recommendation system: similarity covariance
    - Classification: misclassified rate
- ***Privacy vs. Utility***
  - Both mechanisms sacrifice utility to gain privacy
  - ***Tradeoff***: To get the maximal utility in a fixed

63

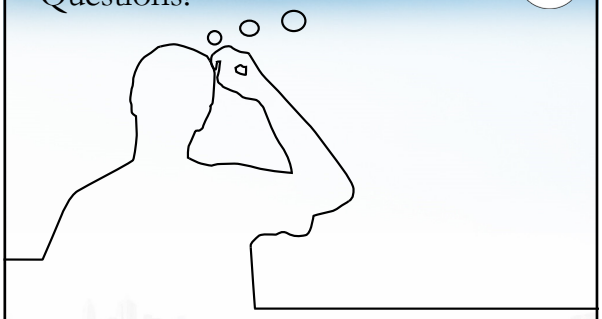
Privacy Preserving Related Reference



- **Privacy Breach on Venue Check-ins:**
  - Huy Quan Vu, Rob Law, and Gang Li. Breach of traveller privacy in location-based social media. **Current Issues in Tourism**, 2019.
- **Privacy Preserving in Data Releasing**
  - T. Zhu, G. Li, W. Zhou, P.S. Yu. *Differential Privacy and Its Applications: Survey*, **IEEE Transactions on Data and Knowledge Engineering**, 2017
  - T. Zhu, G. Li, W. Zhou, P.S. Yu. *Differential Privacy and Its Applications*, Springer 2017
  - T. Zhu, P. Xiong, G. Li, W. Zhou. *Correlated Differential Privacy: Hiding Information in Non-IID Dataset*, **IEEE Transactions on Information Forensics & Security**, 2015, 10(2), 229-242

64

Questions?



65