PRIVACY ISSUES IN GEOSOCIAL NETWORKS
PLAN OF PRESENTATION

• Introduction
• Geosocial networks
• Information Collected
• Privacy Issues and Consequences
• Comparison
• Conclusion
INTRODUCTION
INTRODUCTION

Privacy Issues In Geosocial Networks

https://www.youtube.com/watch?v=hlX_F1VKIdo
INTRODUCTION

Mobile phones and their applications

The biggest companies may know more about us than we do ourselves.
INTRODUCTION

Privacy Issues In Geosocial Networks

Social Network + Location = Locative social media service
Or Location-based social networking
Who has access to our information?

Is it safe to publish it online?

Is our information well protected?
INTRODUCTION

Mobile application “Girls around me”

Foursquare

Facebook

Serial killer
The website “Please Rob Me”* can fetch all the locations related to a Twitter account, showing the danger of publicly shared location data.

* http://pleaserobme.com
One Android user shares his location **5398 times** during **14 days**, with or without his intervention.
“A web-based or mobile-based service that allows users to construct a profile containing some of their geo-located data (along with additional information), connect with other users of the system to share their geo-located data and interact with the content provided by other users (for instance by commenting, replying or rating)”

Gambs, Heen & Potin (2011)
“A comparative privacy analysis of geosocial networks”
“A Location-Based Social Network (LBSN) does not only mean adding a location to an existing social network so that people in the social structure can share location-embedded information, but also consists of the new social structure made up of individuals connected by the interdependency derived from their locations in the physical world as well as their location-tagged media content, such as photos, video, and texts”

Yu Zheng (2012)  
“Computing With Spatial Trajectories”
WHAT IS A GEOSOCIAL NETWORK?

Generating & Consuming

Interaction

Sharing & Understanding

Privacy Issues In Geosocial Networks
Geolocation apps do two things:

1. **Report** your location to other users

2. **Associate** real-world locations (such as restaurants and events) to your location.
CLASSIFICATION OF GSNs: GEOTAGGED-MEDIA-BASED

https://www.flickr.com
CLASSIFICATION OF GSNs : GEOTAGGED-MEDIA-BASED

https://www.panoramio.com
CLASSIFICATION (ZHENG 2011)

- **Geotagged-media-based**: enable users to *add location labels* and *comments* on media contents (text, photos, videos or others.)
  
  Examples: Flickr, Panoramio and Geo-twitter

- **Point-location-driven**: share users *current locations* by checking-in into the places they visit and adding *"tips"* to venues.
  
  Examples: Foursquare
CLASSIFICATION OF GSNs: POINT-LOCATION-DRIVEN

https://foursquare.com
CLASSIFICATION (Zheng 2011)

• Geotagged-media-based: enable users to *add location labels* and *comments* on media contents (text, photos, videos or others.)
  Examples: Flickr, Panoramio and Geo-twitter

• Point-location-driven: share users *current locations* by checking-in into the places they visit and adding “tips” to venues.
  Examples: Foursquare

• Trajectory-centric: provide *point location* and the *detailed path* by connecting the locations of several points.
  Examples: Bikely and SportsDo.
CLASSIFICATION OF GSNs: TRAJEKTORY-CENTRIC

https://www.bikely.com
INFORMATION COLLECTED
Information Collected

User **personal** information

User **location** information
Techniques to get location data from smartphone

Addresses and zip codes can be translated into GPS

Cell Tower
- Connects to the tower with the strongest signal
- Cell tower signals and location are triangulated

Satellite/GPS
- Wi-Fi locations matched with GPS coordinates
- Satellites may have trouble if you are indoors

User-Reported
- Users register for mobile apps

Smartphone
- Requires a data connection

Wi-Fi
- Wi-Fi has to be on

IP Address
- IP address passed through a database

• System collection: users’ location data are collected and revealed *directly* through a *system interface*.

Example: Facebook and its Graph Search engine

• Third party application collection: users’ location are collected by a *third party application*. Gathering users’ information from different sources to build a *complete profile* including personal content and location data.
PRIVACY ISSUES AND CONSEQUENCES
Privacy Issues

• “...the decision of sharing something online is made at the moment”
  (Das and Sahoo 2011)

• “...people's ideas about privacy are malleable depending on the context of interaction”
  (Acquisti - TEDGlobal 2013)

• “people are more willing to divulge sensitive personal information on a social network website than on other sites”
  (Acquisti - TEDGlobal 2013)

• “people disclose information when they see others do it”
  (Acquisti - TEDGlobal 2013)

• “...many people are ready to provide personal information online”
  (Gross and Acquisti 2005)
**PRIVACY ISSUES: OPINIONS OF PRIVACY FROM COMPANIES**

<table>
<thead>
<tr>
<th>Do you agree or disagree with the following statements? Privacy from Companies and Legality</th>
<th>Agree Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>If a website has a privacy policy, that means it will not share my personal information with others.</td>
<td>68%</td>
</tr>
<tr>
<td>I like it when companies use the information I post to decide what products to advertise to me.</td>
<td>28%</td>
</tr>
<tr>
<td>I would like more control over what companies do with the photos and information I post online.</td>
<td>75%</td>
</tr>
<tr>
<td>Companies are not interested in what I say and do online.</td>
<td>39%</td>
</tr>
</tbody>
</table>

*Young Canadians in a Wired World* conducted by MediaSmarts in 2014
### Privacy Issues: Privacy Policy or Terms of Use Agreement

<table>
<thead>
<tr>
<th>Has someone ever read a privacy policy or online terms of use agreement with you and explained what it means?</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, my parent(s) or another person in my family</td>
<td>29%</td>
</tr>
<tr>
<td>Yes, a teacher/guidance counsellor</td>
<td>6%</td>
</tr>
<tr>
<td>Yes, a librarian</td>
<td>2%</td>
</tr>
<tr>
<td>Yes, a coach, instructor, or community leader (for example, Girl Guides, Boy Scouts)</td>
<td>2%</td>
</tr>
<tr>
<td>Yes, someone else</td>
<td>6%</td>
</tr>
<tr>
<td>No</td>
<td>65%</td>
</tr>
</tbody>
</table>

*Young Canadians in a Wired World* conducted by *MediaSmarts* in 2014
**Privacy Issues: Who should be allowed to track location?**

<table>
<thead>
<tr>
<th>Some devices or applications (apps) can track where a person is located (for example, GPS phone, Facebook, Foursquare). Who do you think should be allowed to check and see where YOU are?</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>My friends</td>
<td>39%</td>
</tr>
<tr>
<td>My boyfriend/girlfriend (Gr. 7-11 only)</td>
<td>27%</td>
</tr>
<tr>
<td>My parent(s) and people in my family</td>
<td>69%</td>
</tr>
<tr>
<td>My teacher or principal</td>
<td>8%</td>
</tr>
<tr>
<td>Kids my age I have not met before</td>
<td>2%</td>
</tr>
<tr>
<td>Adults I have not met before</td>
<td>1%</td>
</tr>
<tr>
<td>Anyone who knows me</td>
<td>9%</td>
</tr>
<tr>
<td>The company that owns the site or app</td>
<td>4%</td>
</tr>
<tr>
<td>Marketing companies that want to advertise to me</td>
<td>1%</td>
</tr>
<tr>
<td>The police</td>
<td>35%</td>
</tr>
<tr>
<td>Other</td>
<td>6%</td>
</tr>
<tr>
<td>No one should be allowed to check and see where I am</td>
<td>20%</td>
</tr>
</tbody>
</table>

Young Canadians in a Wired World conducted by MediaSmarts in 2014
Location Privacy Issues (Alrayes and Abdelmoty -2014)

- **Location Data Collection:** gathering and storage of location information and its quality.

- **Location Information Accessibility:** accessibility and visibility of information by other users and third parties of the service (*disclosure of the user’s data*).

- **Location Data Exploitation:** how the user’s location information is used and for what purposes, either by the application itself or any third parties.

- **Location Data Security:** level of protection of the user’s data against the risk of loss or unauthorized access.
Privacy Issues

What information is stored?
Could we know who controls the information?
How securely will it be stored?
How it can later be used or disclosed?
Where will it be stored?
How long it will be stored?
Examples of Consequences

Advantages

Positive Effects

Disadvantages

Negative Consequences

Privacy Issues In Geosocial Networks
ADVANTAGES : CASE 1

Harvard University
Harvard University is more than classrooms and buildings. It’s an interconnected community of people, ideas, and experiences.

Source: http://foursquare.com/Harvard
ADVANTAGES: CASE 2

Privacy Issues In Geosocial Networks

Source: https://es.foursquare.com/historychannel
ADVANTAGES: CASE 3

Cloak 'anti-social' app helps you avoid your friends

While most social networks aim to connect people, one new service seeks to join the growing trend of doing the opposite and help you avoid them.

Cloak uses public location data from other social networks, Foursquare and Instagram, to determine the locations of others you know.

Users can choose to receive an alert when certain people are believed to be nearby.

It is the latest in the recent trend of 'anti-social', or secretive, apps.

Apps such as Snapchat - which deletes photographs and videos seconds after they have been viewed - and Secret - which broadcasts messages anonymously - are growing in popularity.

Likewise WhatsApp, a private-messaging service recently bought by Facebook for $16bn (£11.4bn), indicates a shift back to conducting online conversations in private.

ADVANTAGES : CASE 4

Used by *criminals* to:

- Identify an individual’s present or *predicted future* location
- Cause *harm* others and their property.
- *Burglary* and *theft*
- *Stalking*
- *Kidnapping*
- *Domestic violence*
The **lack of caution** when posting photos, comments and stories + physical location

**Best tools for**

*kidnapping, robbery, rape, dismissal from work, divorce or separation* of the couple, and so on.
"78% of ex-burglars think there is a very good chance that current thieves turn to Facebook, Twitter, and Foursquare to locate empty homes to target for a robbery."

Credit Sesame – 2011

Source: http://www.creditsesame.com/blog/social-media-safety-dont-make-it-easy-for-burglars/
“74% of ex-burglars believe thieves use Google Street View to scope out potential homes before they strike.”

Credit Sesame – 2011

Source: http://www.creditsesame.com/blog/social-media-safety-dont-make-it-easy-for-burglars/
“It is possible to discover user **Points Of Interests (POIs)** by using **inference attacks**: where someone lives, where he works, places where he practices sports, his usual itineraries, etc.”

(Gambs et al. 2010)

“**Only four spatiotemporal points are enough to uniquely identify 95% of the individuals**”

(De Montjoye et al. 2013)
COMPARISON
### Table 1: Categorization of GSNs privacy-preserving works

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Spatial and Temporal Cloaking-based</th>
<th>Location Transformation-based</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmokeScreen</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>Longitude</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>C-Hide&amp;Seek and C-Hide&amp;Hash</td>
<td></td>
<td>•</td>
</tr>
<tr>
<td>Mobishare</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>N-Mobishare</td>
<td>•</td>
<td></td>
</tr>
<tr>
<td>LocX</td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

Table 1: Categorization of GSNs privacy-preserving works
### Table 2: A comparison between different GSNs privacy-preserving works

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Centralization</th>
<th>Implementation complexity</th>
<th>Communication cost</th>
<th>Time cost</th>
<th>Hardware cost</th>
<th>User pre-settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmokeScreen</td>
<td>Yes</td>
<td>F</td>
<td>F</td>
<td>H</td>
<td>F</td>
<td>Yes</td>
</tr>
<tr>
<td>Longitude</td>
<td>Yes</td>
<td>L</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>Yes</td>
</tr>
<tr>
<td>C-Hide&amp;Seek</td>
<td>Yes</td>
<td>F</td>
<td>F</td>
<td>L</td>
<td>F</td>
<td>No</td>
</tr>
<tr>
<td>C-Hide&amp;Hash</td>
<td>Yes</td>
<td>F</td>
<td>F</td>
<td>H</td>
<td>F</td>
<td>No</td>
</tr>
<tr>
<td>Mobishare</td>
<td>No</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>H</td>
<td>Yes</td>
</tr>
<tr>
<td>N-Mobishare</td>
<td>No</td>
<td>F</td>
<td>L</td>
<td>H</td>
<td>F</td>
<td>Yes</td>
</tr>
<tr>
<td>LocX</td>
<td>No</td>
<td>H</td>
<td>L/H</td>
<td>L/H</td>
<td>F</td>
<td>No</td>
</tr>
</tbody>
</table>
**Analysis of Techniques**

- **SmokeScreen**: main disadvantage is the *time cost*. Transforming an opaque identifier to a real identity takes 10 seconds in best cases.

- **Longitude**: performs encryptions and computations *faster* than other techniques.

- **C-Hide&Seek and C-Hide&Hash**: C-Hide&Hash provides a *higher level of privacy* than C-Hide&Seek do, but at the cost of *higher communication and computation costs*. 
ANALYSIS OF TECHNIQUES

• Mobishare,
  • Requires a complexes implementation and an additional hardware to adequately perform.
  • Still immature in terms of privacy preserving.

• LocX:
  • More complicated to implement than other techniques
  • Is the most efficient one in pointing queries.
  • Main weakness is the nearest-neighbor queries: needs too much time and data to properly perform.
CONCLUSION
Applications that are mostly constructed to depend on geo-location services are slowly invading and colonizing our daily life.

They can have access to our addresses and locate the residences of our friends, family and acquaintances.

There's nothing wrong with the use of this type of service as long as the consumers are fully conscious and totally aware of what is happening with their personal information and understand the meaning of disclosing location in terms of security.
CONCLUSION

• Many users are unaware of the scope of geo-location technology and this is why they need to be better informed and less complacent.

• Users can be more circumspect when it comes to sharing data with others.

• All categories of concerned people, policymakers, enterprises and consumers should work together to ensure that sensitive personal information is under control.
Thank you