Security in Computing & Information Technology

Lecture 11

Privacy in the Digital World

Lecture Schedule

Foundations

1. Introduction
2. Vulnerabilities, Threats, Attacks

Basic mechanisms

3. Security mechanisms, Elementary cryptography
4. Authentication
5. Access control

Major computing security areas

6. Operating systems
7. Databases
8. Networks
9. Web
10. Mobile computing

Applications

11. Privacy
12. Internet banking

Lecture Topics

- Cloud security
- Social networks
- Privacy and publicity
- Location-based services

Cloud Computing

THOSE ARE APPLICATIONS... SERVERS... DATABASES... WEBSITES... AND THE BIG FLUFFY ONE IS MY BLOG.
SLANE
co.nz

Image source: http://blogs.msdn.com/b/nzgovtech/archive/2012/05/03/the-new-and-the-old-of-the-cloud.aspx

Security & Privacy in the Cloud

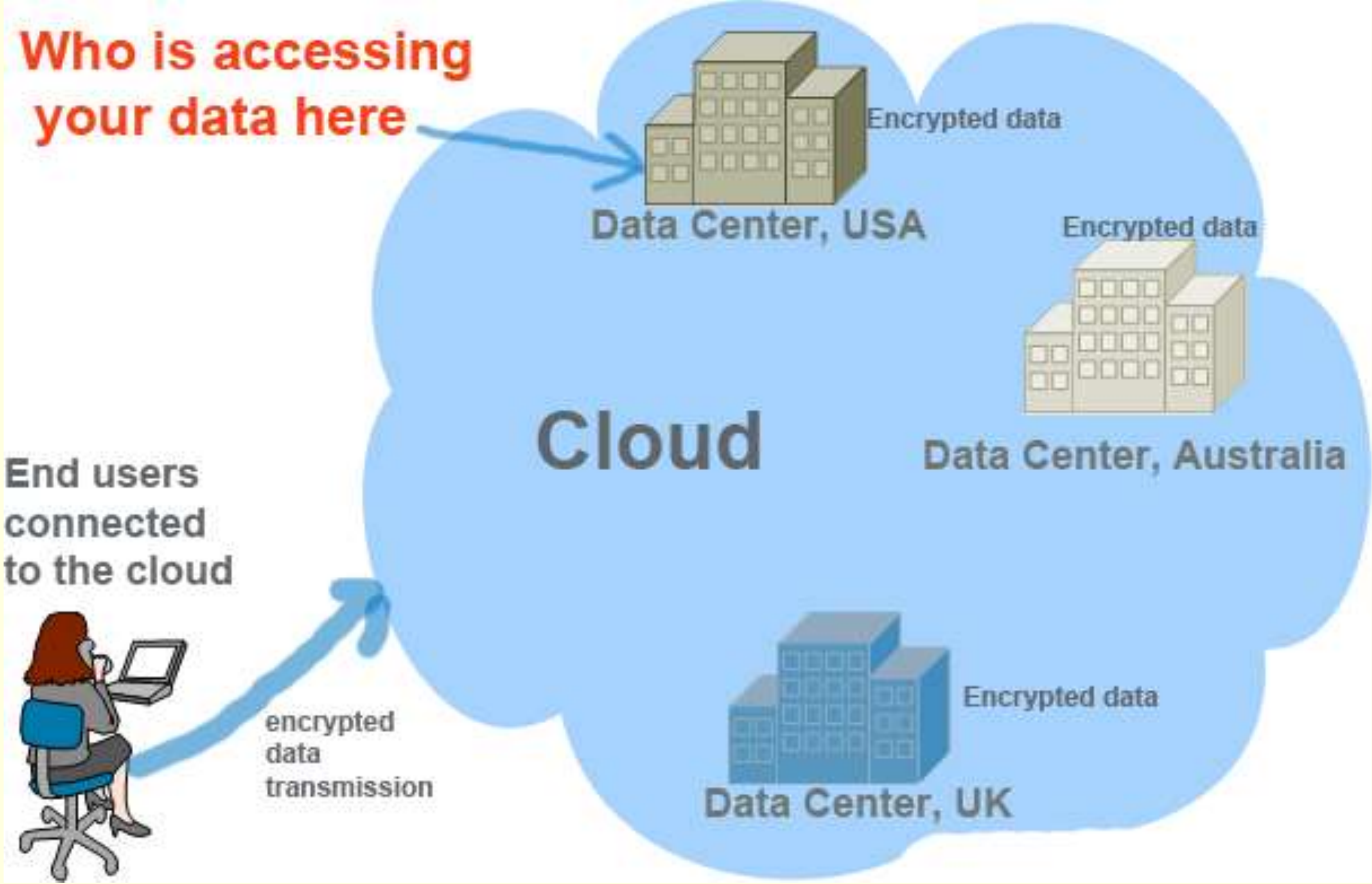


Image source http://securitywing.com/cloud-privacy-issues-questions-users/

Cloud Security & Privacy Concerns

- Shared environment
  - In theory: Users control access
  - In practice: Users have to trust technology not revealed to them by the cloud service provider (CSP)
- Service provider problems
  - Possibility of CSP internal attacks
- Lack of immediate client control
  - Users may not have any say in how/where the data is stored
- Availability
  - Users may experience unforeseen system shutdowns

Solutions for the Cloud

- Data auditing
  - Regular checking of data accuracy & consistency
  - Main issues
    - Timely data anomaly detection
    - Third-party verification without breaching privacy
- Encryption
  - Main issues
    - Performance loss
    - Encryption key management
  - Special encryption methods
    - Searchable encryption
    - Homomorphic encryption

      Allows mathematical operations on encrypted data

      Currently can do addition and multiplication

      Has prohibitively high overhead

Privacy on the Web (1)

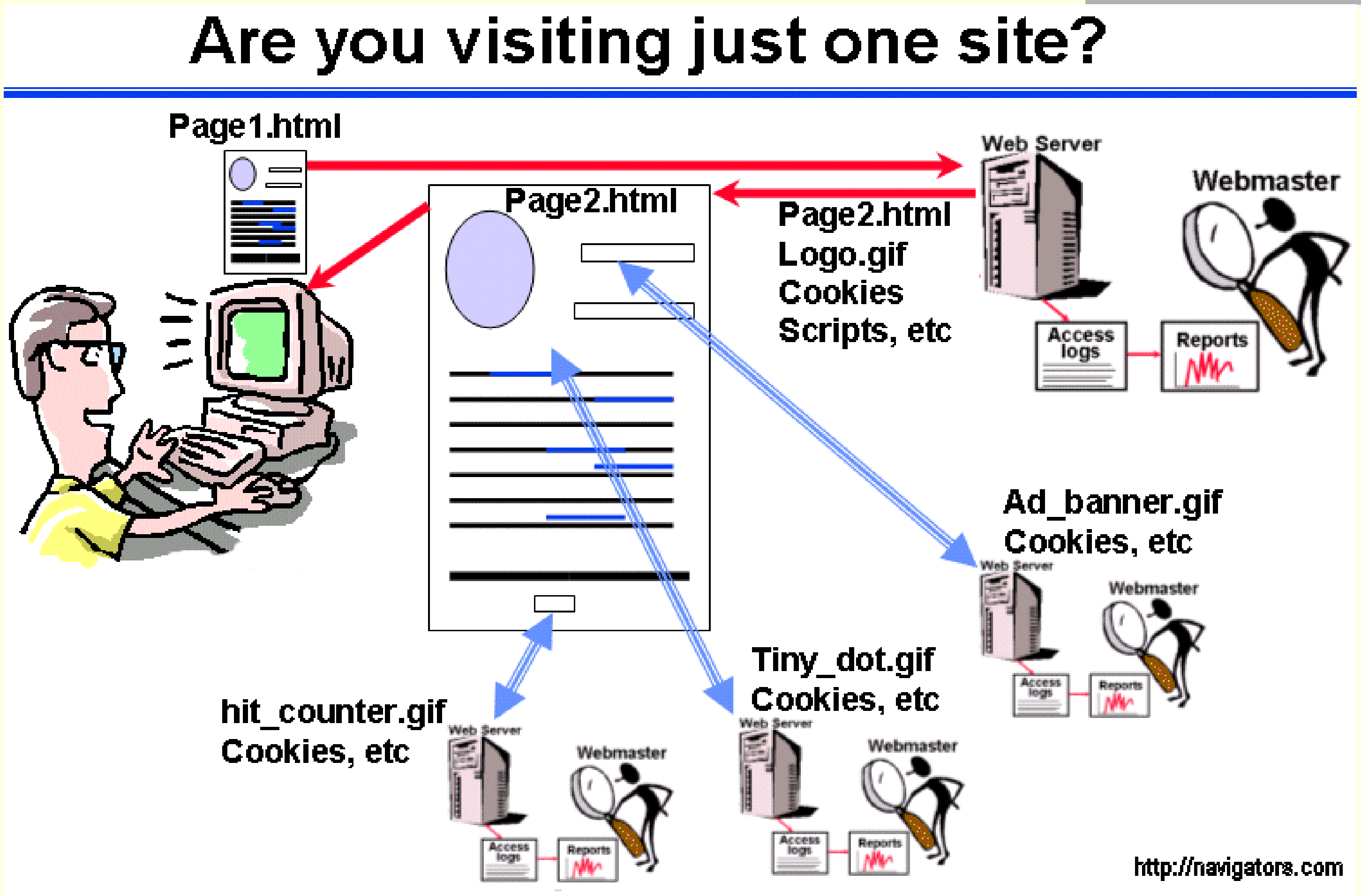
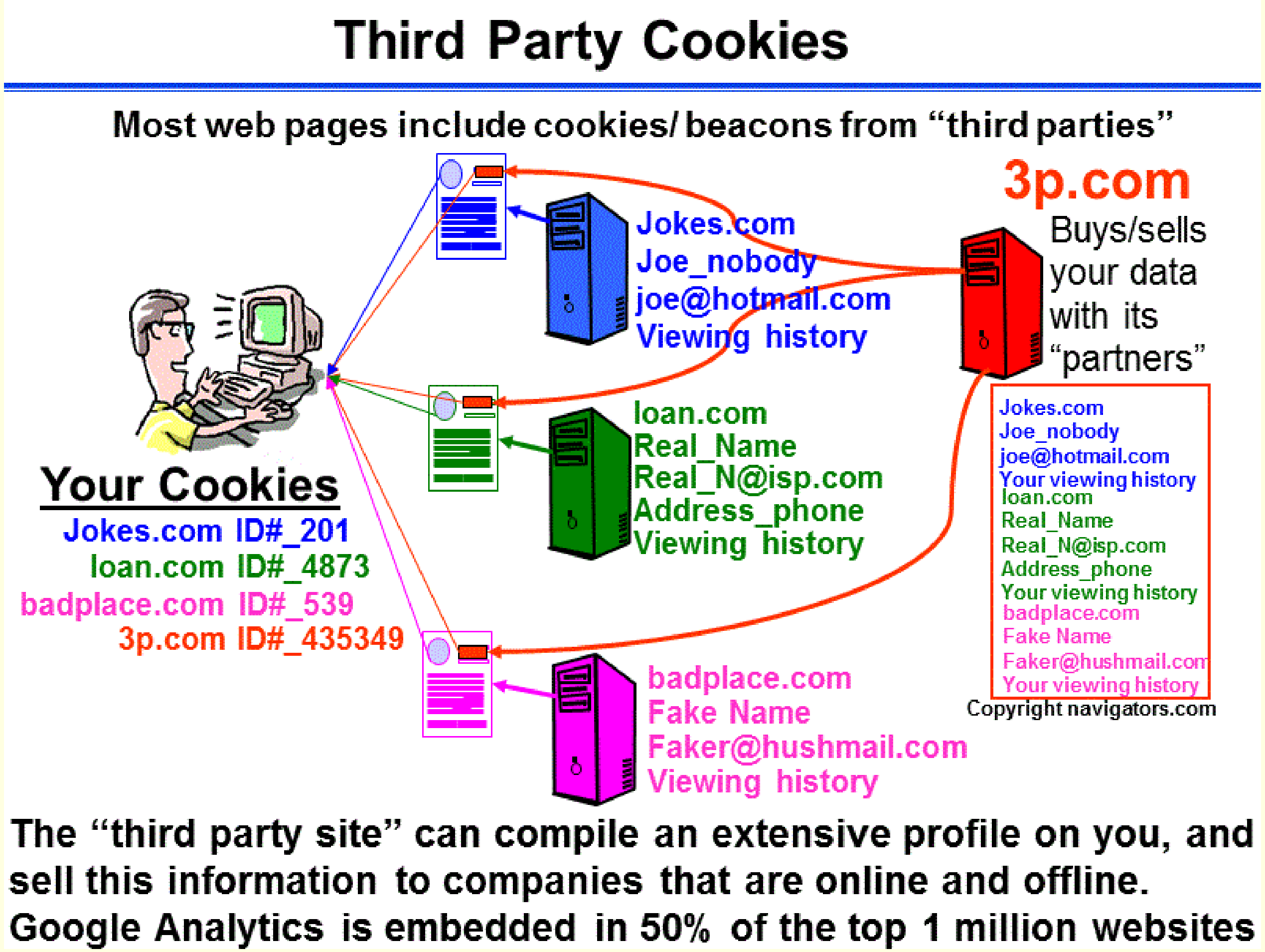


Image source: http://www.navigators.com/cookies.html/

Privacy on the Web (2)



Third Party Cookies

Most web pages include cookies/ beacons from "third parties"

The "third party site" can compile an extensive profile on you, and sell this information to companies that are online and offline.

Google Analytics is embedded in 50% of the top 1 million websites

Image source: http://www.navigators.com/cookies.html/

Social Networks (SNs)

- People want to communicate and maintain relationships
  - Means: Social networks
- Internet and Web-based social networks have become very popular
  - Chat rooms, messaging sites, profile-centric sites, etc
- The sites provide a bounded communication platform based on each user's
  - public or semi-public personal profile
  - list of other users (friends) with whom information is shared
- Both profile and list of friends are accessible by site users

Types of SNs

- General purpose networks (Facebook, MySpace, Badoo, Netlog …)
  - Communication and interaction between users
  - Anybody can join
  - Cater for a variety of interests
- Niche networks
  - Focus on a special activity, geographical region, linguistic group, etc
    - LinkedIn – professional contacts
    - classmates.com – old school friends
    - Orkut – Brasilian community (50%)
    - Ning – users create their own social websites and networks
    - etc

Typical Use of SN Sites

- Create personal profiles
- Post
  - photographs (e.g. Instagram)
  - messages (e.g. WhatsApp)
  - announcements (e.g. AskFM)
- Send and receive messages
- Link to pages of others
- Information is not checked for reliability

  Can cause problem e.g. with professional sites (LinkedIn)

World Map of Social Networks

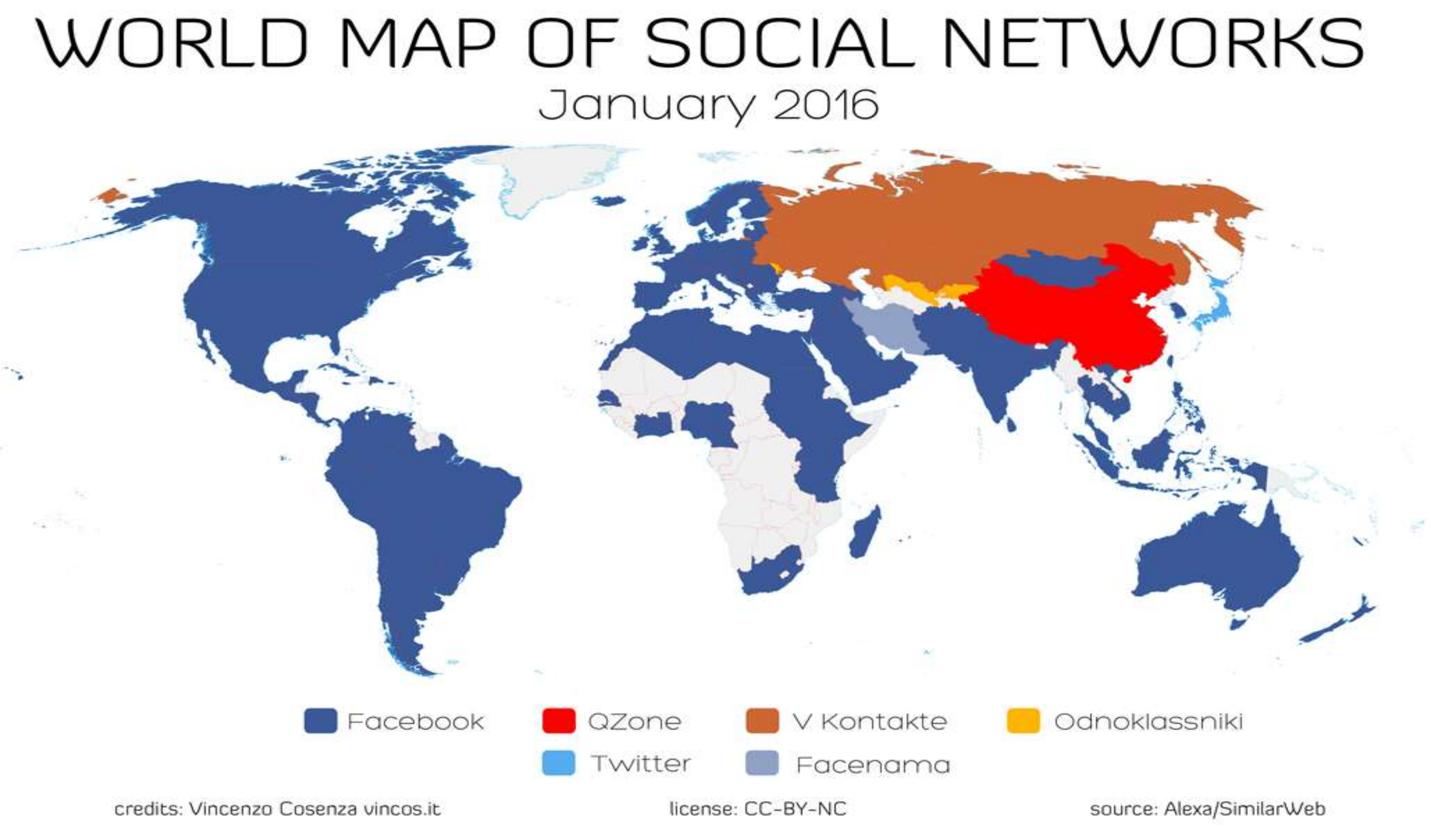


Image source: https://www.dreamgrow.com/world-map-of-social-networks/

Social Relationships on the Internet

- Social networks were designed for weak ties
  - On-line is less stressful than face-to-face meeting
  - People may “open up” over the computer
- Connections are characterised by various familiarities
- Security support is currently limited
- Users often don’t even use existing security features

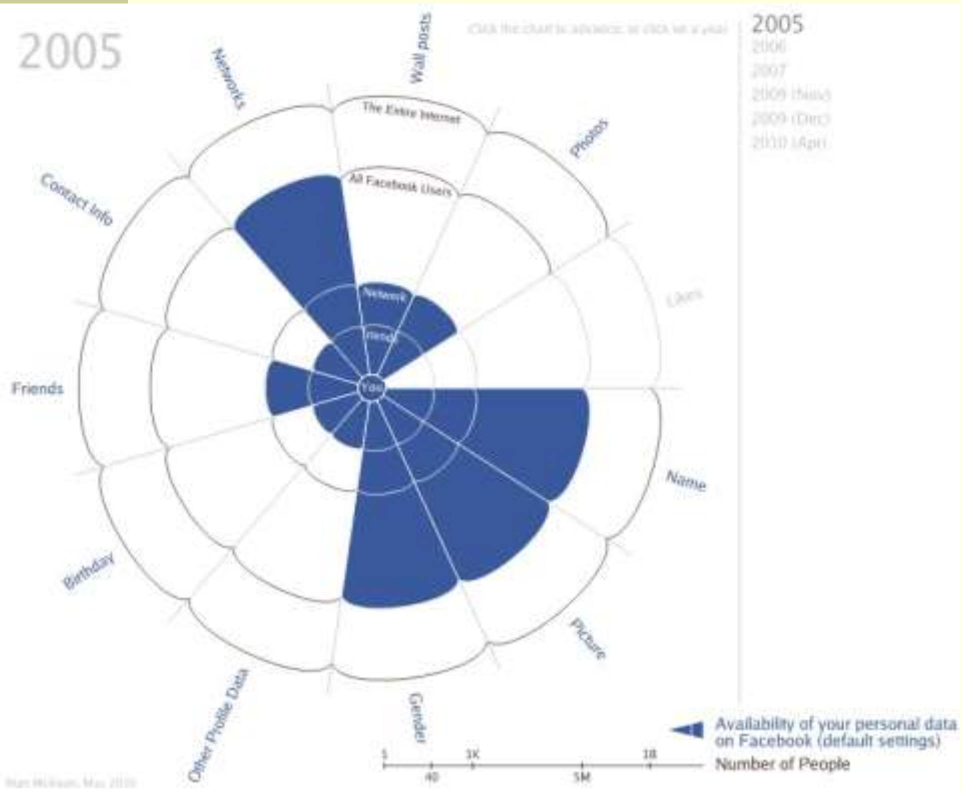
SN Security and Privacy

- Social networks raise a number of security and privacy issues, both technical and social
- We focus on the technical or technically related issues only
- You still need to be aware of the social issues, even though they are not covered here

SN Privacy Policies

- Theory
  - Tells users about the site's practices and obligations
  - Users then can decide what features are acceptable, they can opt in or opt out
  - The presence of such a policy increases user trust
- Practice
  - Policies are
    - hard to find
    - take a long time to read
    - can change without notice
  - Example
    - Facebook: Large web page (http://www.facebook.com/policy.php)

Evolution of Publicly Available Data on Facebook



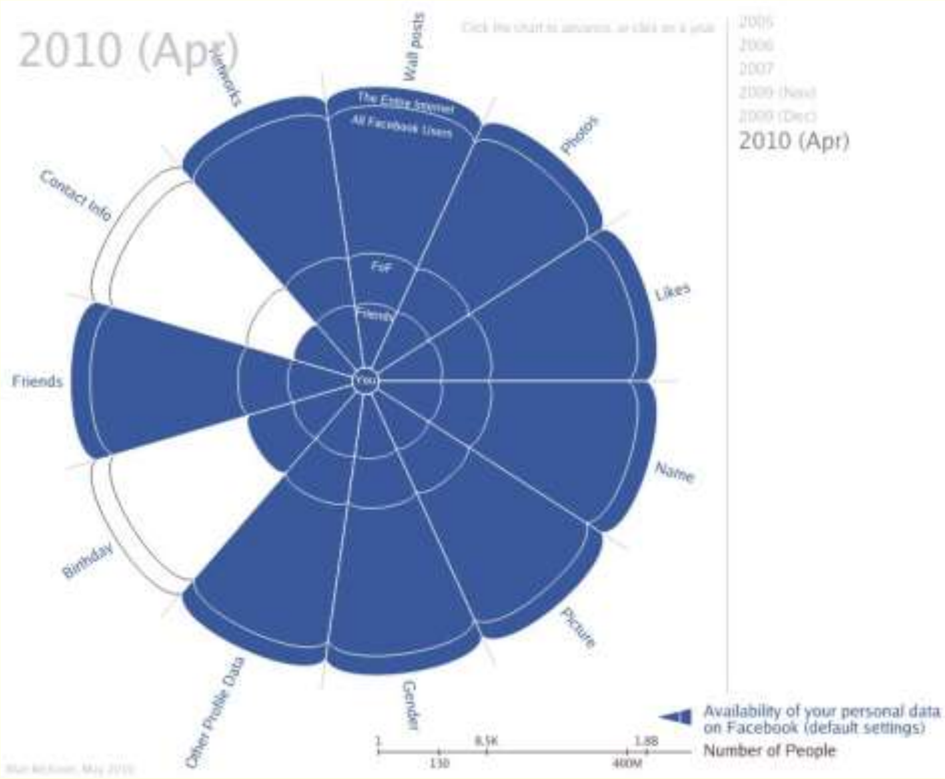
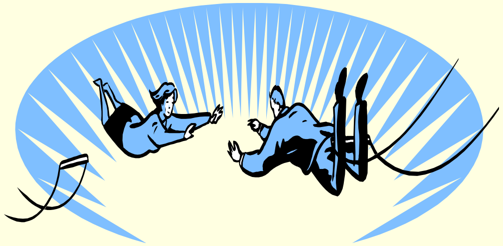


Image source: http://mattmckeon.com/facebook-privacy/

Trust in Social Networks



- Many features are hard-coded in the system
  - Permissions, access to data
  - Access categories, structure
    - E.g. public, open to friends, open to selected friends
  - Joining a group
    - Most sites require bidirectional confirmation of friendship, some don't
- Simplistic modelling
  - A connection may not mean friendship in everyday sense
  - Membership and trust are binary (no parameter to describe closeness, role, …)

Security in Social Networks

- Exploiting social relationships
  - Malicious banner ads
  - Phishing
  - Custom scripts: users can add “applications” to enhance their profiles
- Predefined groups (no flexibility, “one size fits all”)
  - Transparency leading to loss of privacy

    At some sites group member lists are visible, at others users can opt out of showing their friends
- Some sites allow customisation of user group permissions (e.g. phpFox)
  - Fine tuning access permissions can be cumbersome

    People may prefer predefined solutions

Privacy Dangers in SNs

- No remedy for private data disclosure
  - Credit cards can be cancelled if compromised
  - Your personal data cannot be cancelled even if compromised
- Potential information leak to
  - other users
  - third parties
  - platform providers
- Data aggregation
  - Single sign-on is increasingly used between SN sites
  - Greater potential to combine private data

Privacy Protection

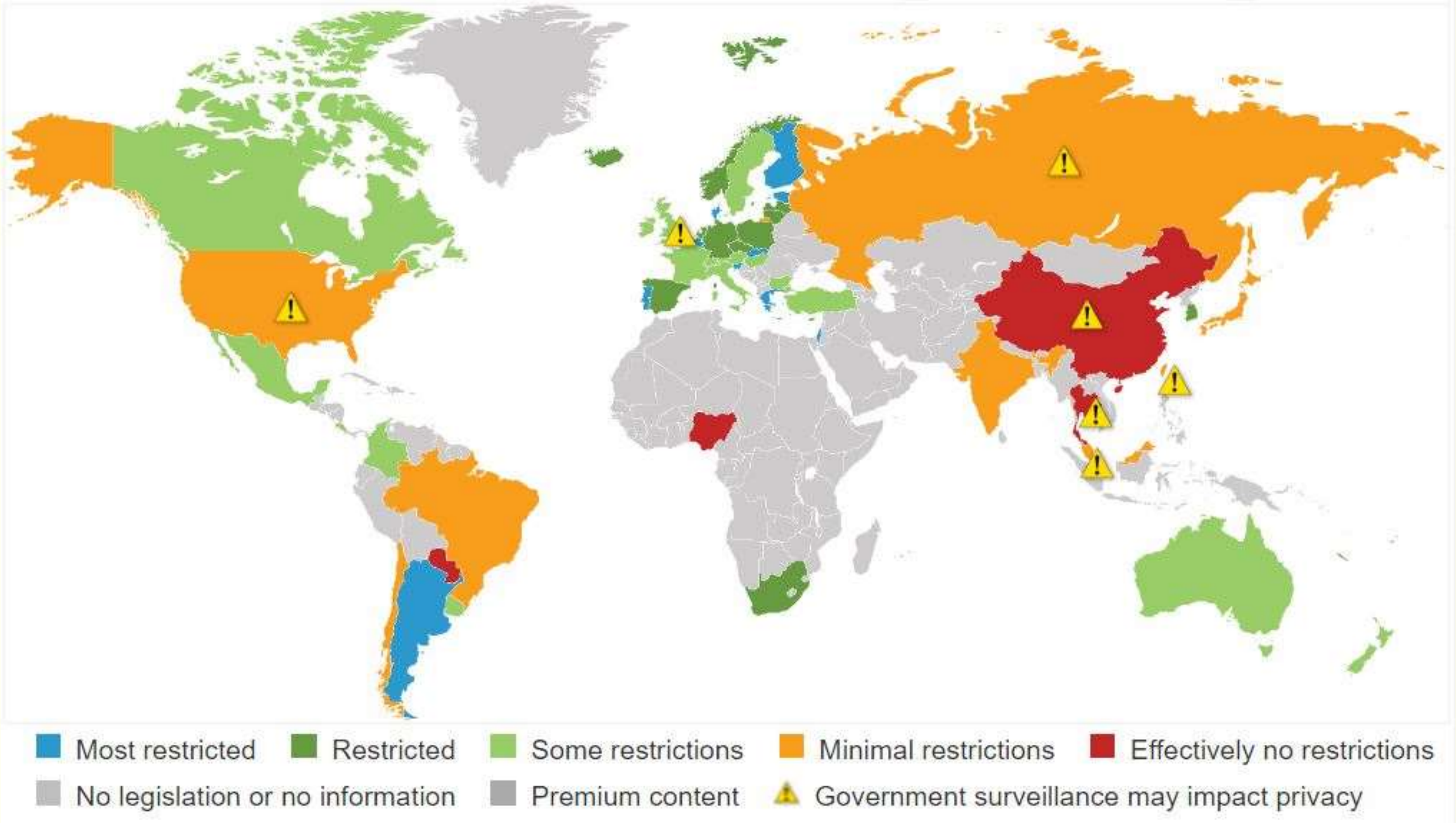

🟦 Most restricted
🟩 Restricted
🟩 Some restrictions
🟧 Minimal restrictions
🟥 Effectively no restrictions
⬜ No legislation or no information
⬛ Premium content
⚠ Government surveillance may impact privacy

Image source: http://heatmap.forrestertools.com/

Privacy and Publicity

- To remain safe
  - Theory: you can be safe by observing all privacy rules
  - Practice: you need to set tens of flags, and hitting a wrong key once can still cancel the safe setting
- Legally: published information can be considered intention to communicate with large audience
- Ways of revealing information
  - Direct publishing
  - Indirect publishing

Direct Publishing

- Revealing personally identifiable information
  - Issues
  - Scope in time
    - Data retention: data may be available after deletion
      - http://justdelete.me/ ranks web services according to deletion difficulty
  - Scope in space
    - Who can access the information
- Searchable attributes
  - Some sites are crawled by search engines (Friendster, Tribe.net)
    - Content is visible to non-members (outsiders)
  - Can reveal connections not explicitly stated in data
    - Example: face recognition software
    - Windows Live photo gallery "automatically recognises who's who in your photos" http://www.facebook.com/notes/livesidenet/windows-live-wave-4-photo-gallery-with-facial-recognition-and-photo-fuse/391538288056

Indirect Publishing (1)

- Privacy risk by friends
  - Friends can publish your private data

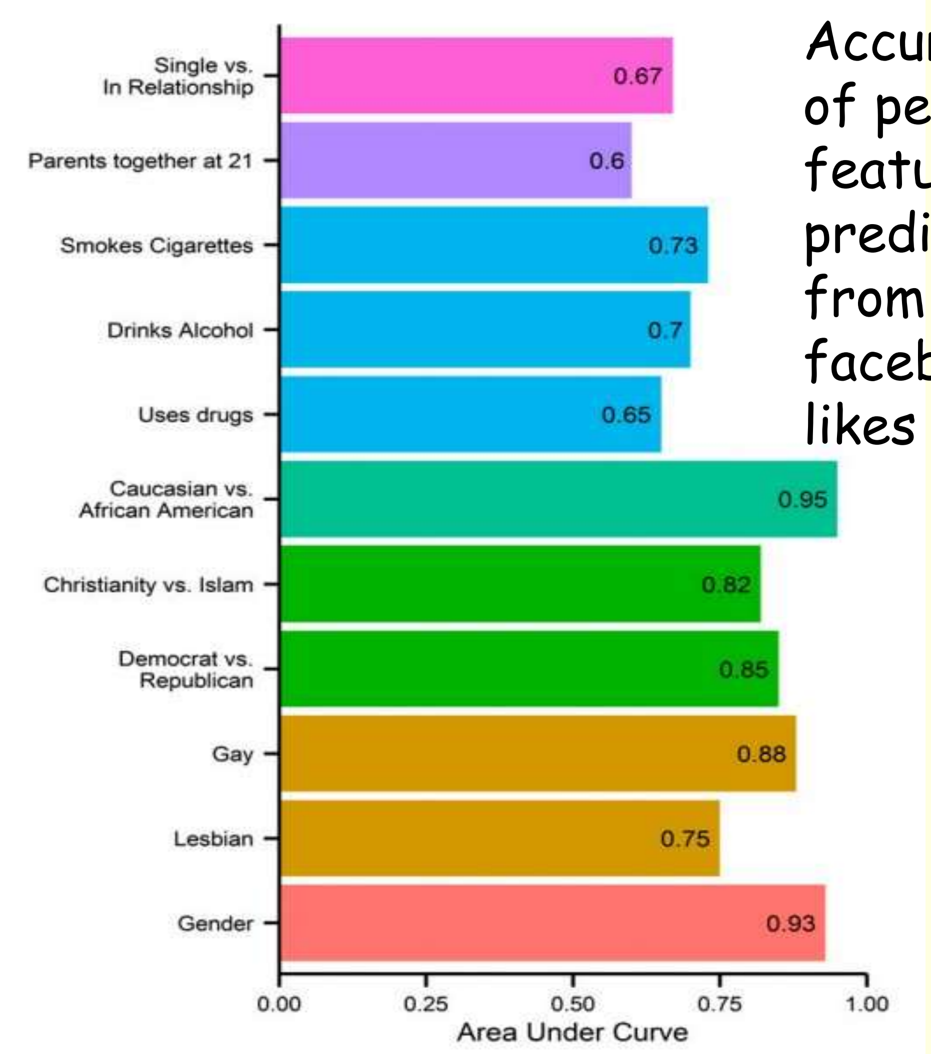
    E.g. network of friends
    - Photos showing you
    - Your name as a Facebook friend, even though you marked your list of friends as private in your entry
  - Others can infer attributes via friends or friends' attributes

    E.g. check the attribute values of all friends and select the most frequent one (over 50% success rate!)
  - Once published, cannot be retracted
    - Site may keep deleted data

      (Facebook does/did, Snapchat has automatic deletion)
    - Others may have copied the data before you deleted it

Indirect Publishing (2)

- Private traits and attributes are predictable from digital footprints



Accuracy of personal feature prediction from facebook likes

Source http://www.pnas.org/content/early/2013/03/06/1218772110.full.pdf+html

Indirect Publishing (3)

- Privacy risk by third party software

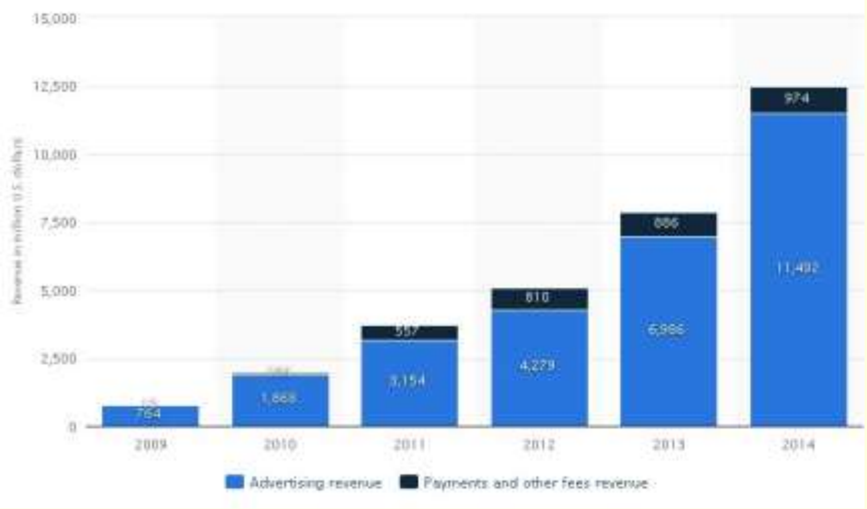
  Example: Facebook applications

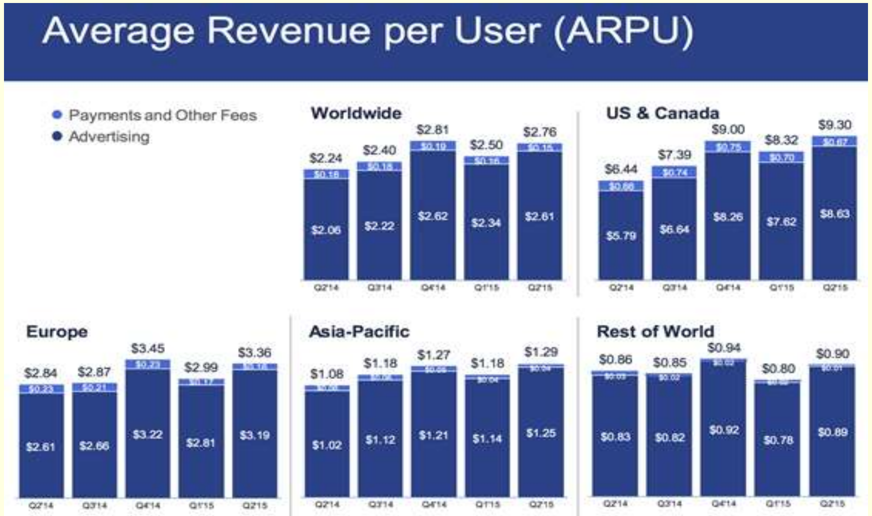
  - When a user installs an application, the application acquires the privileges of the profile owner (Sensitive data are not made available to third party applications, but Facebook "cannot guarantee that [third parties] will follow our rules")
  - Many of these applications are "marketing businesses built on top of the idea that third parties can get access to data on Facebook."

http://www.fastcompany.com/articles/2008/10/social-networking-security.html

SN Sites – Business Model

- Advertising is big business
- Targeted advertising based on personal interests is more effective
  - User profiles provide ample information about users' interests
- Example: Facebook revenue





Source: http://www.statista.com/statistics/267031/facebooks-annual-revenue-by-segment/

SN Sites, Privacy and Marketing

- User activity monitoring
  - SN sites monitor user activities to gather information about interest
  - User monitoring can go beyond the actual SN site

    E.g. Facebook monitors user activity via cookies even after logging out (http://nikcub-static02.appspot.com/logging-out-of-facebook-is-not-enough)
- Leaking user data
  - E.g. applications may harvest email addresses

Example: Targeted Advertising

- Facebook
  (https://en-gb.facebook.com/business/help/337584869654348/?helpref=hc_fnav)
  - Targeting options
    - Location, Age & gender, Language, Interests, Behaviours, Connections
  - Ad tracking
    - Facebook pixel

      Allows to track if a person saw the ad and then completed a particular action (e.g. purchase)

Responsibility of Privacy

- People want to share certain information about themselves
- The information posted can be used for compiling data for legitimate and not-so-legitimate purposes

  Examples
  - Companies using 'social' groups for marketing
  - Employers monitoring SN sites
  - Criminals looking for identity theft victim
- Balance of trust and usage goals

Employers and SN Sites

- Employers monitor SN sites to
  - learn employee's off-duty behaviour (private life)

    e.g. medical condition, sexual preferences, alcohol or drug use
  - prevent leaking of company information
  - screen job applicants

    e.g. checking photographs, communication skills, political affiliations or activities
  - …
- Automatic tools easily search out information
- Employee/applicant has no defence, as the information was published

SN Sites and Crime

- SN sites are attractive targets for criminals
  - Facebook has over 400 million users
- Blackmail
  - Incriminating pictures, anything up to personal details can be used
  - (e.g. 18 yo posing as a female collected nude pictures from male classmates)
- Impostors
  - Masquerading as someone else
- Scam
- Identity theft
  - Personal data mining applications
  - Games (or other applications) can collect personal data
- Users' irresponsible actions
  - E.g. messages "left home and checked in less than a minute ago: I'm at New York Penn Station" by users whose home address is published

Law Enforcement

- Evidence can be collected from SN sites to
  - reveal personal communication
  - establish personal relations
  - reveal motives
  - provide location information (e.g. IP logs)
  - prove and disprove alibis
- SN sites usually
  - are cooperative with law enforcement agencies
  - require legal process (e.g. search warrants) to retrieve private messages

Service Providers against Law Enforcement

- Service providers and equipment makers try to retain customer confidence by publicly resisting information release
  - Apple defied court order to unlock terrorists' phone (Feb 2016)
    - US government: Apple had agreed to assist before the case became public
  - Facebook refused to comply with court order to hand over drug traffickers' data to police
    - Vice president in Brazil arrested for refusing to share WhatsApp data (March 2016)

Glitches and Publishing Private Data

Glitch: short-lived fault in a system

- Programs may (and usually do) contain bugs
- Some bugs may result in privacy breach

  Examples
  - Telstra delivers SMS to random recipients (Feb 2017)
  - Facebook security flaw allowed people to eavesdrop on their friends' live chats (May 2010)
  - Facebook delivered emails to the wrong mailbox (Feb 2010)
  - Facebook reveals data marked confidential (DOB) (July 2008)
  - Blippy
    - Exposed "raw data" (e.g. airline reservation code – combined with surname it can be used to check in) (Apr 2010)
- Private data are often published by hackers
  - E.g. SnapchatDB published 4.6 million user names and numbers (Dec 2013)

Basic Security Tips

- Don't post anything you wouldn't mind telling a complete stranger
  - In reality that's the potential for access
  - Real friends would know most of that information anyway
- Be careful who you add as a "friend,"
  - No way of verifying a user's actual identity online
- Use common sense in general
  - Any complex system has some vulnerabilities, and SN sites are no exception

Location and Privacy

- Location-Based Services
  - Location-based information

    E.g. “find a restaurant near me”
  - Location-based billing

    E.g. roaming
  - Emergency services
  - Tracking

    E.g. vehicle movements for fleet operators

Location-Based Services (LBS)

Technology

- Positioning
  - Most frequently used method: Global positioning system (GPS)
  - Other methods (triangulation, phone cell information, etc) can also be used
- Geographic information systems (GIS)
  - Processes map data (e.g. streets) and points of interest (e.g. restaurants)
- Location management function
  - Processes positioning and GIS data for LBS applications

Summary

- Social networks over the Internet implement simplistic relationships
- Published personal data
  - is not retractable
  - can used by many