



# Privatnost na društvenim mrežama

**Institut Ruđer Bošković, kolokvij knjižnice**  
Zagreb, 11. ožujka 2015.

**Filip Vlašić**  
Nacionalni CERT, CARNet

# Što su osobni podaci?

- EU komisija:
  - „Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, your bank details, your posts on social networking websites, your medical information, or your computer’s IP address.”
  - [http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1\\_en.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf)
  - Sud Europske unije 13. svibnja 2014. donio je presudu o „pravu na zaborav”
- RH:
  - Zakon o zaštiti osobnih podataka
  - „Osobni podatak je svaka informacija koja se odnosi na identificiranu fizičku osobu ili fizičku osobu koja se može identificirati (u daljnjem tekstu: ispitanik); osoba koja se može identificirati je osoba čiji se identitet može utvrditi izravno ili neizravno, posebno na osnovi identifikacijskog broja ili jednog ili više obilježja specifičnih za njezin fizički, psihološki, mentalni, gospodarski, kulturni ili socijalni identitet.”

# Tko želi naše osobne podatke?



Država

- uprava
- sigurnost



Tvrtke

- marketing
- **zarada**



Zlonam.

- kriminal
- **ostalo**



# Uvjeti korištenja

- „**Terms and Conditions**”
- nalazimo ih ne samo kod web usluga nego bilo kojeg softvera kojeg imamo na računalu
- procjena: prosječnom korisniku bi godišnje bilo potrebno **180 sati** da pročita svaki TaC

## Terms and Conditions

### USER AGREEMENT

All use of the \_\_\_\_\_ .com Web pages is subject to the terms and conditions set forth below. By accessing and using any portion of \_\_\_\_\_ .com, you agree and accept the terms and conditions described below. If you do not agree with any of these terms and conditions, please do not continue using \_\_\_\_\_ .com. We reserve the right to change the terms of this User Agreement. Changes will be posted at [http://www.\\_\\_\\_\\_\\_.com/TermsAndConditions.aspx](http://www._____.com/TermsAndConditions.aspx), and will become effective immediately upon posting.

### DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY

ALL THE INFORMATION CONTAINED ON THIS WEB SITE IS PROVIDED "AS IS" WITHOUT ANY WARRANTIES OR GUARANTEES OF ANY KIND. THIS WEB SITE MAY CONTAIN ADVICE, OPINIONS AND STATEMENTS OF VARIOUS INFORMATION AND CONTENT PROVIDERS. HOWEVER, THIS WEB SITE IS FOR INFORMATIONAL PURPOSES ONLY. RELIANCE ON SUCH INFORMATION IS AT YOUR OWN RISK.

\_\_\_\_\_ THEREFORE MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE PERFORMANCE OR MERCHANTABILITY OF THE PRODUCTS OR SERVICES REFERRED TO ON THIS WEB SITE. TO THE EXTENT PERMITTED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES, INCLUDING THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON INFRINGEMENT, ARE HEREBY EXCLUDED.

IN NO EVENT SHALL \_\_\_\_\_ BE LIABLE FOR ANY DAMAGE TO HARDWARE OR SOFTWARE BY ANYONE ACCESSING THIS WEB SITE; OR FOR LOSS OF BUSINESS OR PROFITS; OR FOR ANY CONSEQUENTIAL, INCIDENTAL, PUNITIVE, OR SIMILAR DAMAGES; OR FOR CLAIMS OF DAMAGES MADE BY ANY PARTY USING THE INFORMATION CONTAINED ON THIS WEB SITE FOR ANY CAUSE WHATSOEVER, REGARDLESS OF THE FORM OF ACTION.

IN NO EVENT SHALL \_\_\_\_\_ BE LIABLE FOR ANY DAMAGE TO HARDWARE OR SOFTWARE BY ANYONE ACCESSING A THIRD PARTY WEBSITE THROUGH OUR WEB SITE; OR FOR LOSS OF BUSINESS OR PROFITS; OR FOR ANY CONSEQUENTIAL, INCIDENTAL, PUNITIVE, OR SIMILAR DAMAGES; OR FOR CLAIMS OF DAMAGES MADE BY ANY PARTY USING THE INFORMATION CONTAINED ON A THIRD PARTY WEB SITE FOR ANY CAUSE WHATSOEVER, REGARDLESS OF THE FORM OF ACTION.

WE CANNOT ENSURE THAT YOU WILL BE SATISFIED WITH ANY PRODUCTS OR SERVICES THAT YOU PURCHASE FROM A THIRD PARTY THROUGH OUR WEBSITE. WE DO NOT ENDORSE ANY PRODUCT OR SERVICE OFFERED ON THIS WEB SITE. WE HAVE NOT TAKEN ANY STEPS TO CONFIRM THE ACCURACY OR RELIABILITY OF ANY PRODUCT, SERVICE OR INFORMATION CONTAINED ON ANY THIRD PARTY WEB SITE.

\_\_\_\_\_ MAKES NO WARRANTIES OR REPRESENTATIONS AS TO THE INFORMATION PROVIDED BY THIRD PARTIES OR TO THE PERFORMANCE OR MERCHANTABILITY OF THE PRODUCTS OR SERVICES REFERRED TO ON THIS WEB SITE. TO THE EXTENT PERMITTED BY APPLICABLE LAW, ALL IMPLIED WARRANTIES, INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE HEREBY DISCLAIMED. WE DO NOT MAKE ANY REPRESENTATIONS OR WARRANTIES AS TO THE PRIVACY OR SECURITY OF ANY INFORMATION (INCLUDING CREDIT CARD AND OTHER PERSONALLY IDENTIFIABLE INFORMATION) YOU MAY BE REQUESTED TO GIVE A THIRD PARTY.

# Gamestation Aprilili

- online dućan računalnih igara, odlučio je kao prvoaprilsku šalu 2010., u svoj TAC ugraditi odredbu kako kupac pristaje prodati svoju dušu
- rezultat: 88% (7,500) korisnika je to učinilo



# Društvene mreže u Hrvatskoj

- Facebook
  - **1,6 milijuna** korisnika (internetworldstats.com)
  - prosječni korisnik (2013.):
    - 25 minuta dnevno (13 spajanja)
    - 229 „prijatelja“
- LinkedIn, Instagram, Twitter, Tumblr, Google+
- **WhatsUp**, Viber, Facebook Messenger ...
- Steam ...



# Rizici

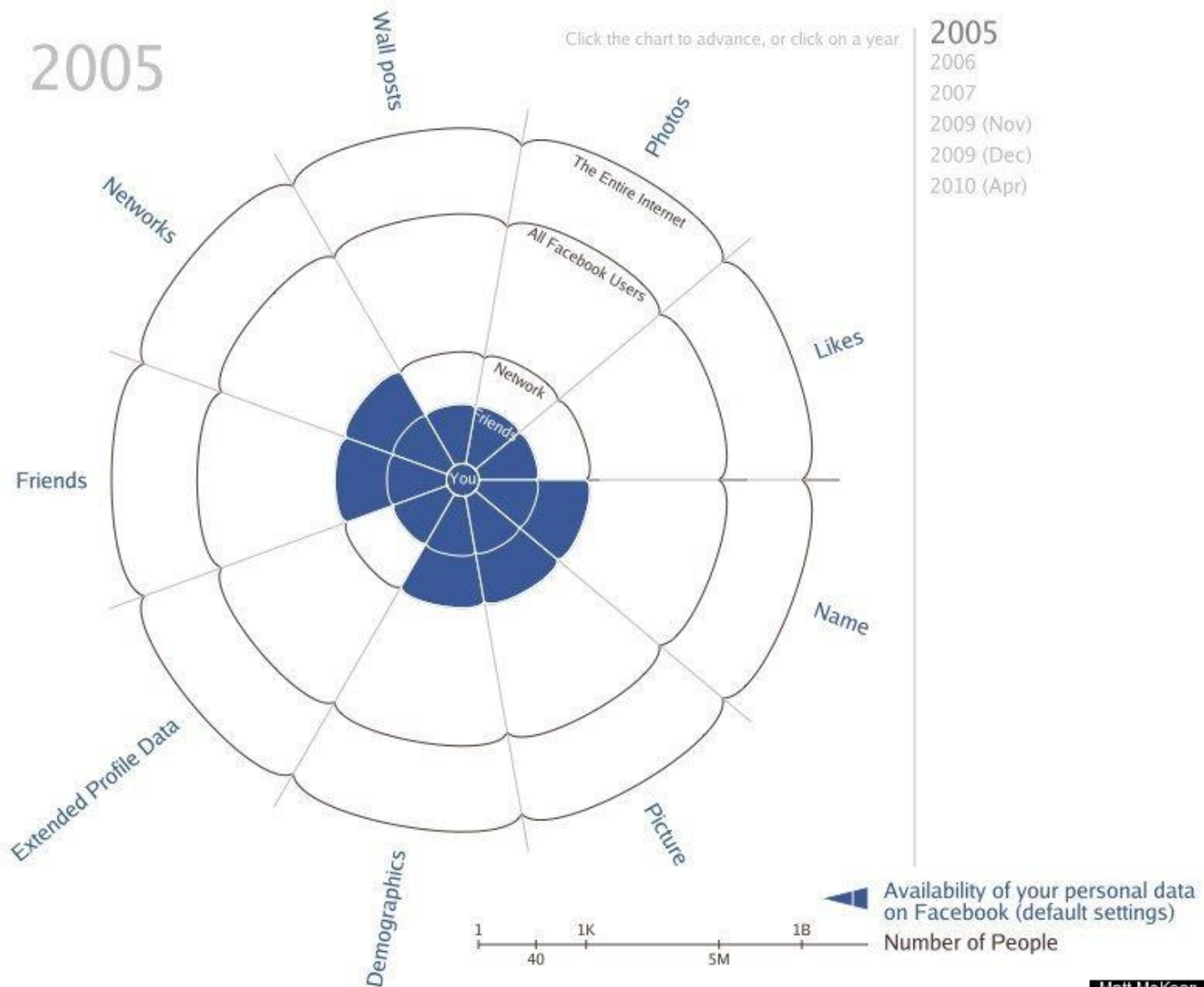
- registracijom na društvenu mrežu, prihvaćamo njezina „**pravila igre**” - ta pravila su labavo definirana kao i u stvarnom životu
- društvene mreže su kompanije koje, kao i svaka druga, maksimiziraju svoj **profit** te moraju pronaći na čemu će zarađivati
- društvenost na Internetu podrazumijeva i zlouporabu kao i u stvarnom životu
- možemo sami sebi narušiti ugled
- **mobilne** društvene mreže su **najrizičnije**



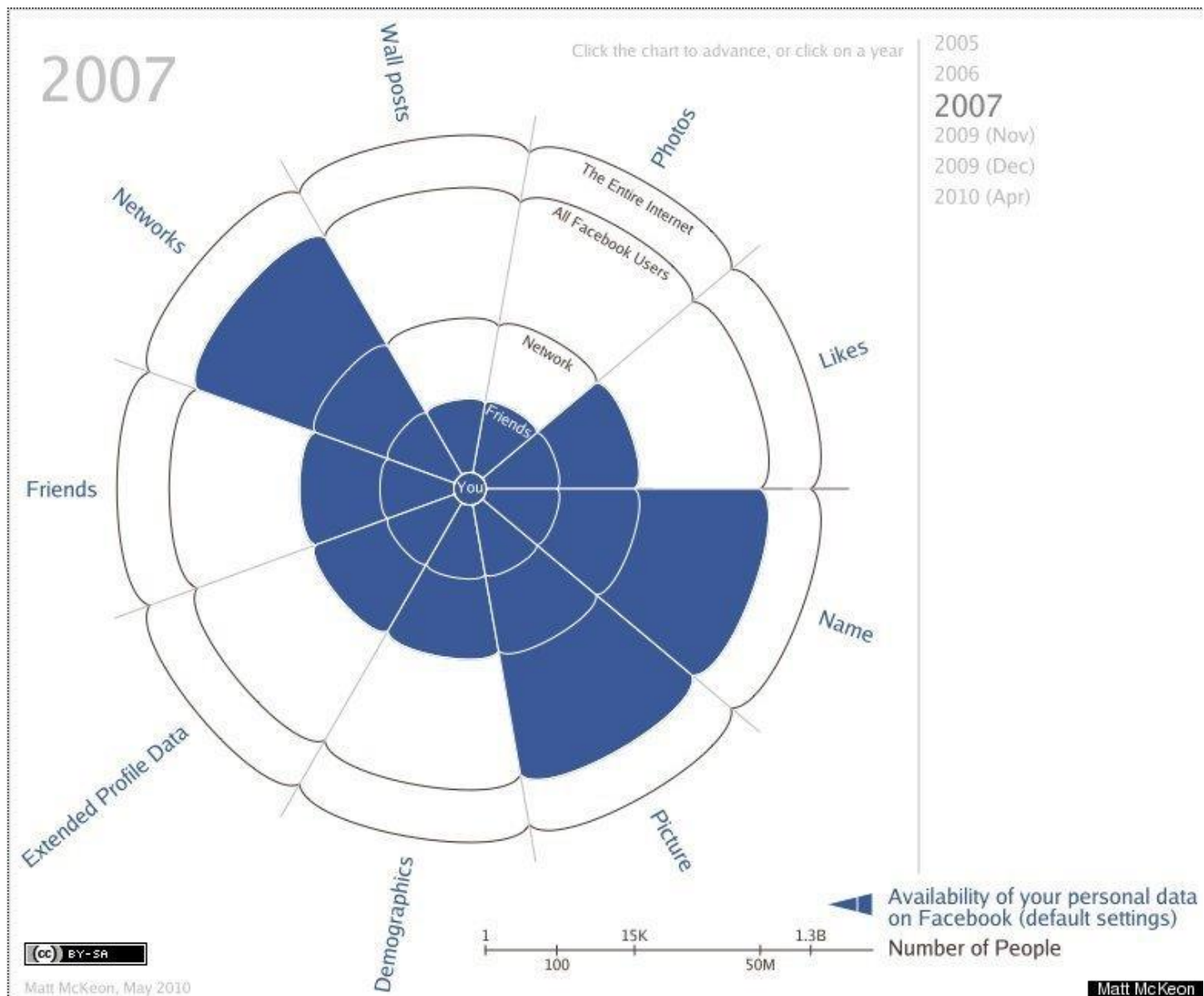
facebook



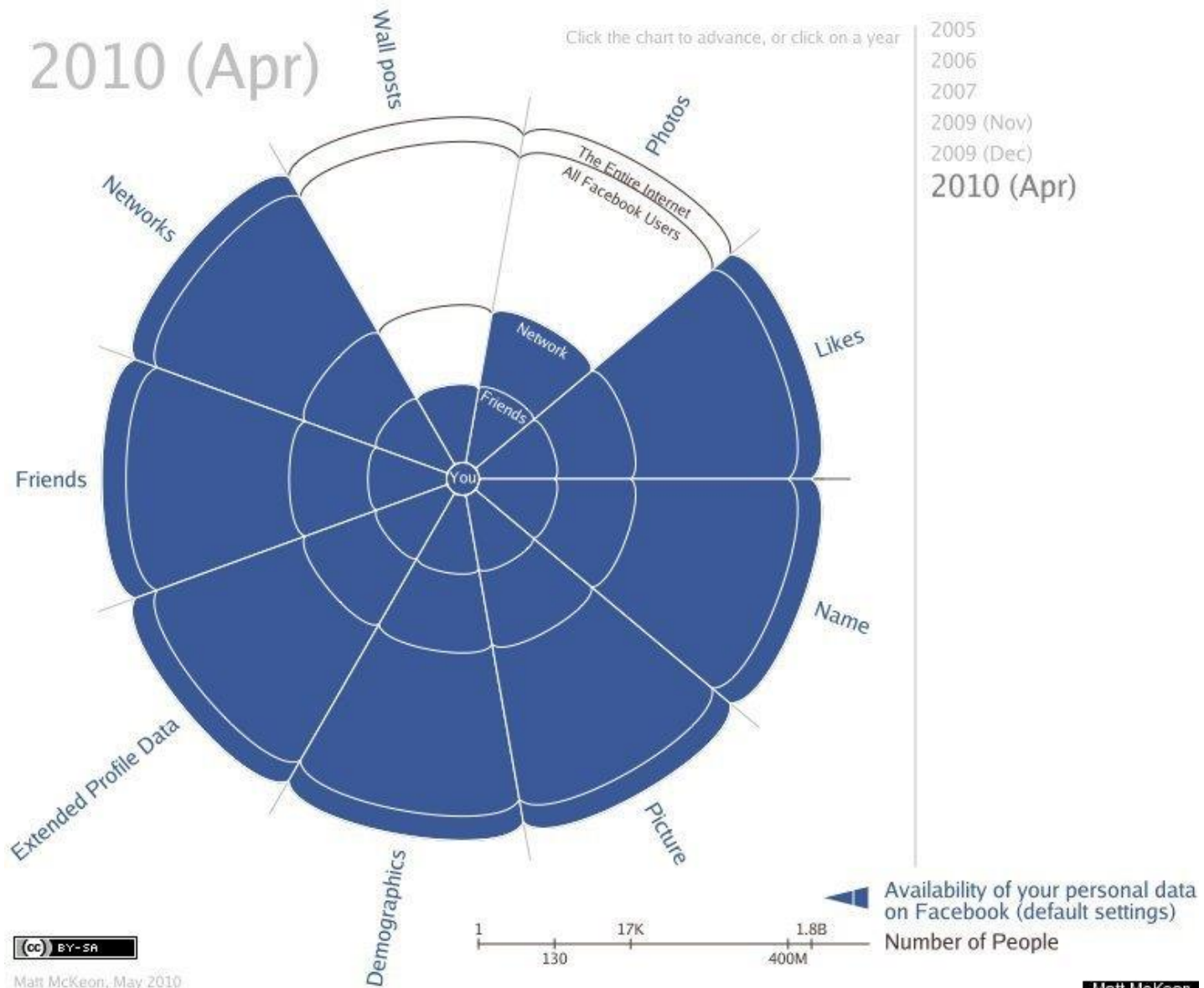
# Dostupnost podataka s Facebooka



# Dostupnost podataka s Facebooka



# Dostupnost podataka s Facebooka



# Politika privatnosti na Facebooku

- <https://www.facebook.com/about/privacy/your-info>, politika privatnosti
- kome će bit dostupni podatci koje ostavljamo na profilima drugih, ovisi o **njihovim** postavkama !
- Facebook i različiti Internet oglašivači međusobno **dijele informacije** (ovo uključuje i GPS lokacije) o vama

# Podaci koje obično dijelimo

- ime i prezime, mjesto i datum rođenja, spol
- mjesto prebivališta, email, telefon
- trenutna i prošla zaposlenja
- veze, kontakti (adresar) i prijatelji
- politička i vjerska stajališta
- seksualna orijentacija
- jezici kojima se znamo služiti
- knjige koje smo pročitali, filmovi, glazba ...

- hrana, restorani i kafići koje volimo
- odjeća i robne marke
- omiljeni sportovi, sportaši i klubovi
- aktivnosti i događanja
- mjesta koja smo posjetili
- veliki životni događaji
- mreže i grupe
- postovi na zidu



# Ali to nije sve ...

- pogledani video zapisi, web stranice, komentari koji nam se sviđaju, ispunjene ankete
- prijatelji s kojima smo na fotografijama i s kojima se često družimo
- zahtjevi za prijateljstvom (odbijeni, raskinuti)
- tvrtke koje nam se sviđaju
- koliko ste često „online“

# Ni to nije sve ...

- stranice i aplikacije koje smo izradili/koristili
- točne geolokacije s kojima pristupamo mreži
- IP adrese
- TV, film ili koncert kojeg trenutno gledamo
- profili s kojima imamo najviše interakcije
- reklame koje gledamo

# Facebook sees 24% uptick in government requests for user data

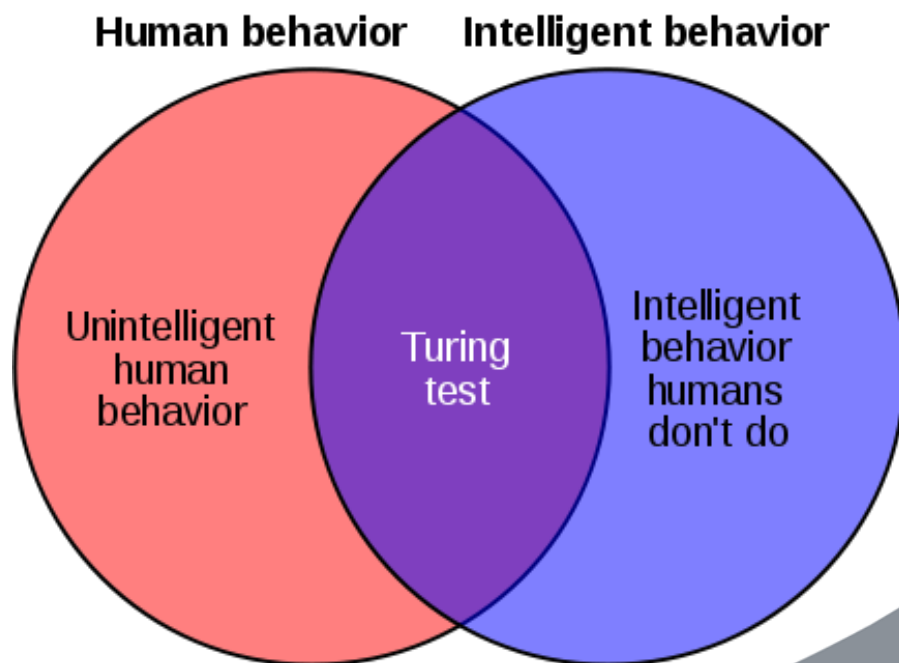
During the first half of the year, the social network received 15,433 requests for data in the US alone.

by [Rachel King](#)  [@rachelking](#) / November 4, 2014 2:43 PM PST

# Inteligentno korištenje !?

- Boshmaf, Muslukhov, Beznosov, Ripeanu: „The Socialbot Network: When Bots Socialize for Fame and Money”, University of British Columbia, Vancouver, 2011.

- Turingov test ----->



# Zašto je teško spriječiti „curenje“ podataka?

- tvrtke ostvaruju zaradu zahvaljujući tim podacima
- „Kada je usluga besplatna, **ti** si zapravo usluga“
- tehnička rješenja sve sofisticiranija => teško spriječiti sigurnosne propuste („rupe“)
- tehnički uređaji i softver ostavljaju mnogo „tragova“
- **ljudski faktor** – najčešći uzrok propusta
- sigurnost (čitaj: inženjeri) košta

# U međuvremenu ...

Adrian Bridgwater

March 10, 2015

## Updated: Facebook Login hijacking tool offered to black hat hackers

Share this article:    

*Penetration testing company Sakurity has openly named and blamed Facebook over a security vulnerability that it says exists on websites with a Facebook login option.*

In a direct call to black hat hackers, Sakurity has created **RECONNECT** as a ready to use tool to hijack accounts on websites including Booking.com, Bit.ly, About.me, Stumbleupon, Angel.co, Mashable.com, Vimeo and many others.

"Feel free to copy and modify [the RECONNECT] source code," says Sakurity founder Egor Homakov. "Facebook refused to fix this issue one year ago, unfortunately it's time to take it to the next level and give black hats this simple tool."

Facebook denies that it has refused to fix the issue, emphasising that it evaluates the trade-offs entailed in making changes. A Facebook spokesman told *SCMagazineUK.com* via email: "This is a well-understood behaviour. Site developers using Login can prevent this issue by following our best practices and using the 'state' parameter we provide for OAuth Login. We've also implemented several changes to help prevent login CSRF and are evaluating others while aiming to preserve necessary functionality for a large number of sites that rely upon Facebook Login."



Facebook Login hijacking tool offered to black hat hackers

# Primjer - WhatsUp

- sigurnosni istraživač Maikel Zweerink u veljači 2015. je razvio tehniku i alat za praćenje online statusa korisnika (mobilnog telefona)
- **WhatsSpy** - demonstracija

# Zlouporabe

- narušavanje ugleda
- uhođenje
- ucjenjivanje
- krađa identiteta
- nanošenje financijske štete
- stvaranje raznih drugih neugodnosti ...



## Facebook Login

### Account Inaccessible

This account is in a special memorial state. If you have any questions or concerns, please visit the Help Center for further information.

Login as:



John Herrman



# Podaci koje treba posebno zaštititi

- **bolje je spriječiti nego liječiti**
- kontakt informacije (telefonski broj itd.), adresa, datum rođenja
- bilo koji osobni podaci koje su poznati jedino nama ili užem krugu ljudi (obitelji)
- lokacijske podatke
- (nepoćudne) fotografije

# Zaštita

- zahtijeva trud i vrijeme
- nikad 100%



DRUGO IZDANJE

# ZAŠTITITE PRIVATNOST NA FACEBOOKU

Saznajte o opasnostima kojima se izlažete prilikom postavljanja osobnih podataka i sadržaja na najpopularniju društvenu mrežu te kako podesiti svoj profil na Fejsu tako da čuva privatnost

LISTOPAD 2014.



**CARNet**  
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA  
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni  
**CERT+**

## Opasnosti Facebooka



# Obratiti se za pomoć Facebooku

- <https://www.facebook.com/help/>



Manage Your Password



See What's New on Facebook



Learn the Privacy Basics



Review Our Safety Resources



Report an Issue



Discover Games & Apps