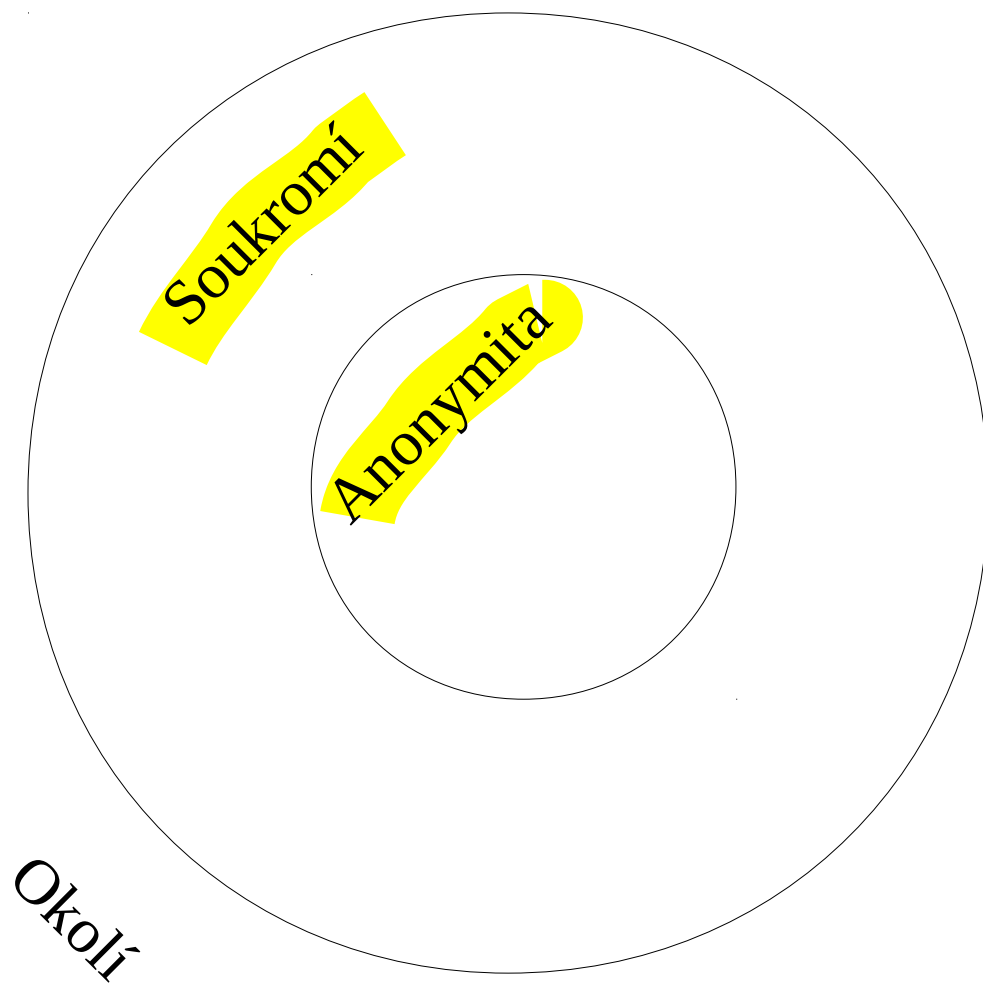
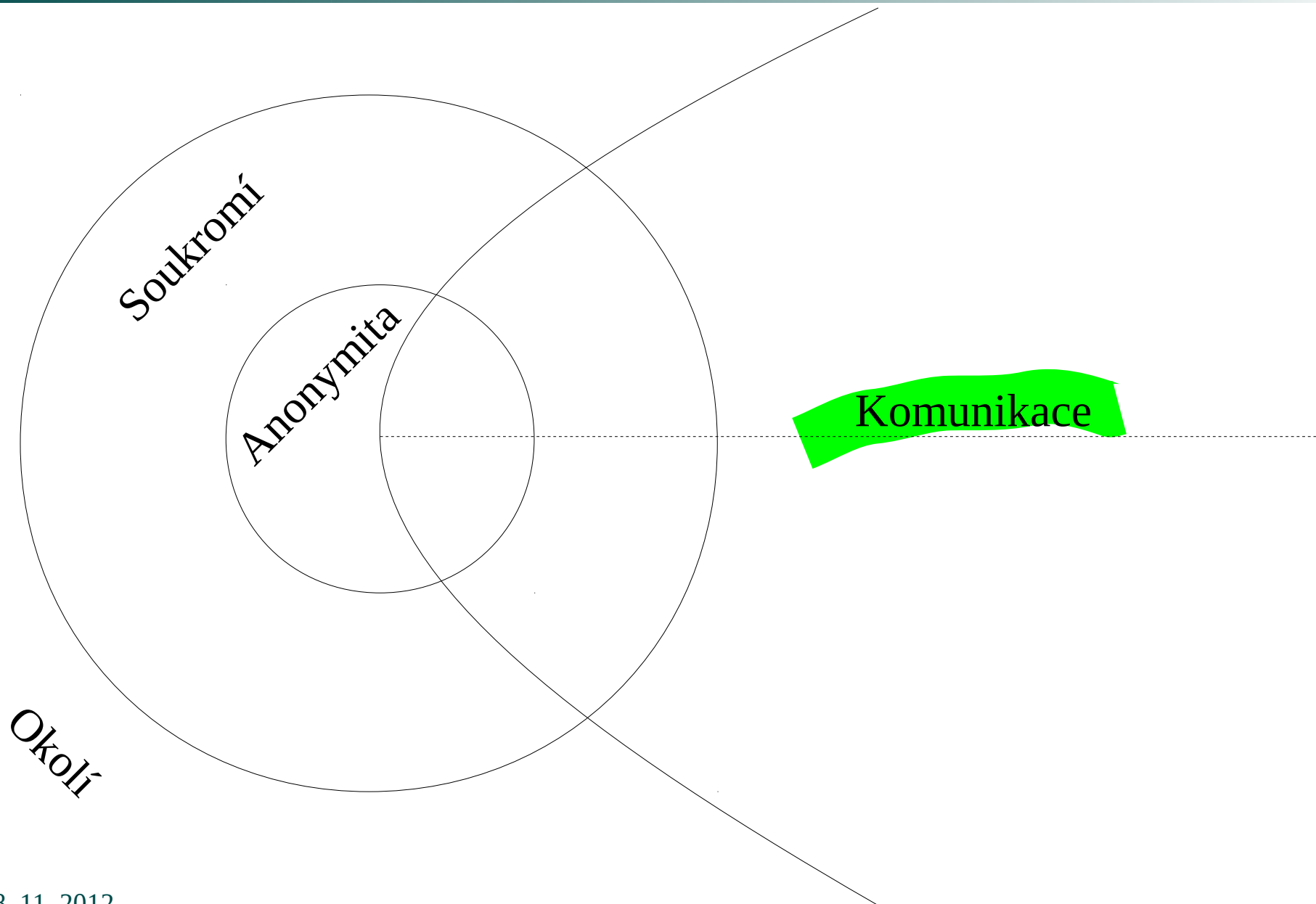


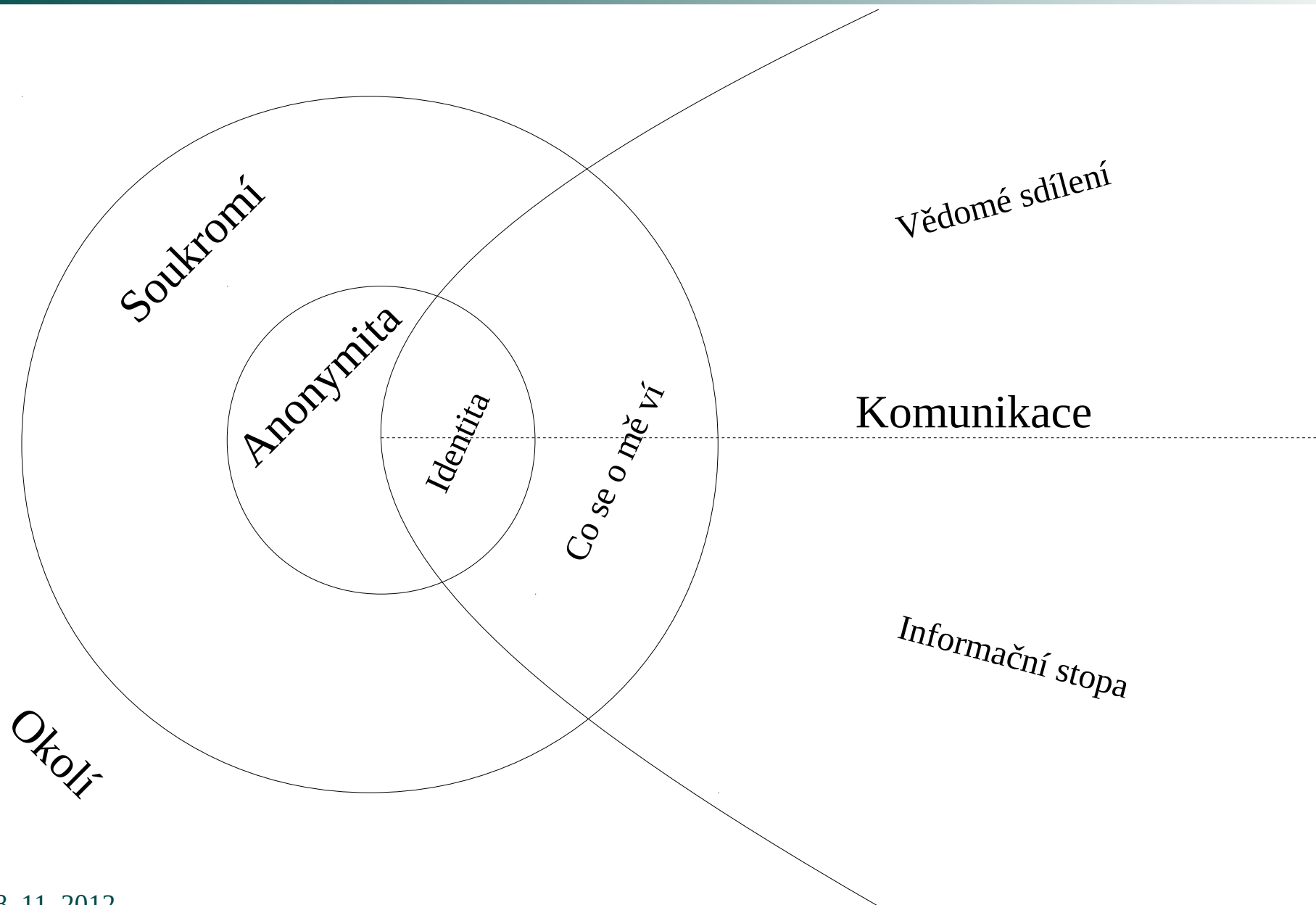
Já, anonym



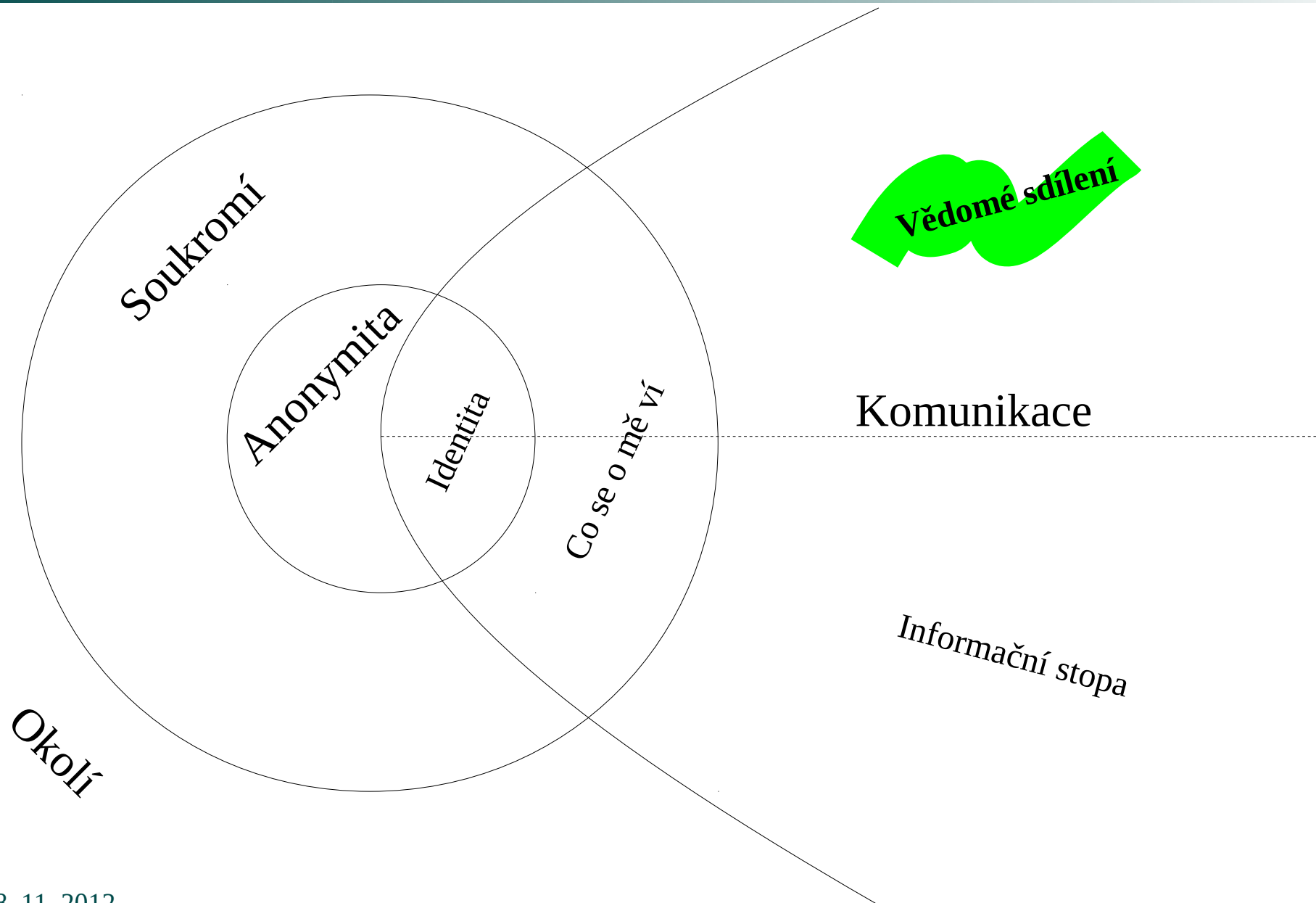
Pavel Kácha
ph@cesnet.cz
CESNET, z. s. p. o.







Vědomé sdílení



Kdo jsme

-   
 - Osobní stránky, blog, CV
 - Skryté stránky – robots.txt, zpětné odkazy, webmail
 - Cloud   
 - Freemail  
 - Odkazy, komentáře
 - CZ.NIC, RIPE
- ```
inetnum: 195.113.134.128 - 195.113.134.255
netname: CESNET-BB2
descr: CESNET, z.s.p.o.
descr: Prague 6
country: CZ
admin-c: VN2-RIPE
tech-c: VN2-RIPE
status: ASSIGNED PA
mnt-by: TENCZ-MNT
mnt-lower: TENCZ-MNT
remarks: Please report network abuse -> abuse@cesnet.cz
source: RIPE # Filtered
```

# Hledání vazeb

- Přezdívky, neobvyklá jména
- Fotografie (zpětné hledání – TinEye, Google Goggles)



- PGP keystore

```
uid Pavel Kacha <ph@rook.cz>
sig sig3 2B2663F8 2002-04-09 _____ [selfsig]
sig sig 687DA204 2002-04-09 _____ Pavel Kácha (pharook) <ph@cesnet.cz>
sig sig 163DF9EB 2002-04-09 _____ Pavel Kůcha (pharook) <ph@cesnet.cz>
sig sig CA57AD7C 2005-06-15 2005-06-29 _____ PGP Global Directory Verification Key
sig sig 9CAA8579 2008-11-20 _____ CESNET-CERTS <certs@cesnet.cz>
sig sig 8ECA352E 2008-11-23 _____ CESNET NIC <nic@ces.net>

uid Pavel Kacha <ph@cesnet.cz>
sig sig3 2B2663F8 2002-04-09 _____ [selfsig]
sig sig 687DA204 2002-04-09 _____ Pavel Kácha (pharook) <ph@cesnet.cz>
sig sig 163DF9EB 2002-04-09 _____ Pavel Kůcha (pharook) <ph@cesnet.cz>
sig sig CA57AD7C 2004-12-30 2005-01-13 _____ PGP Global Directory Verification Key
sig sig 9CAA8579 2008-11-20 _____ CESNET-CERTS <certs@cesnet.cz>
sig sig 8ECA352E 2008-11-23 _____ CESNET NIC <nic@ces.net>
```

# Identifikovatelné objekty

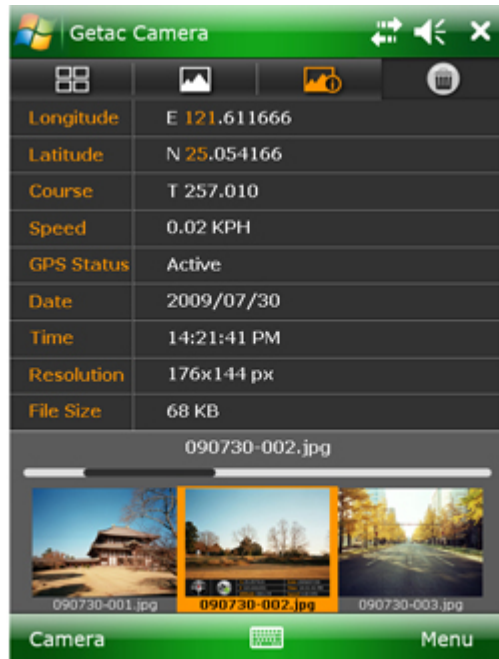




-  

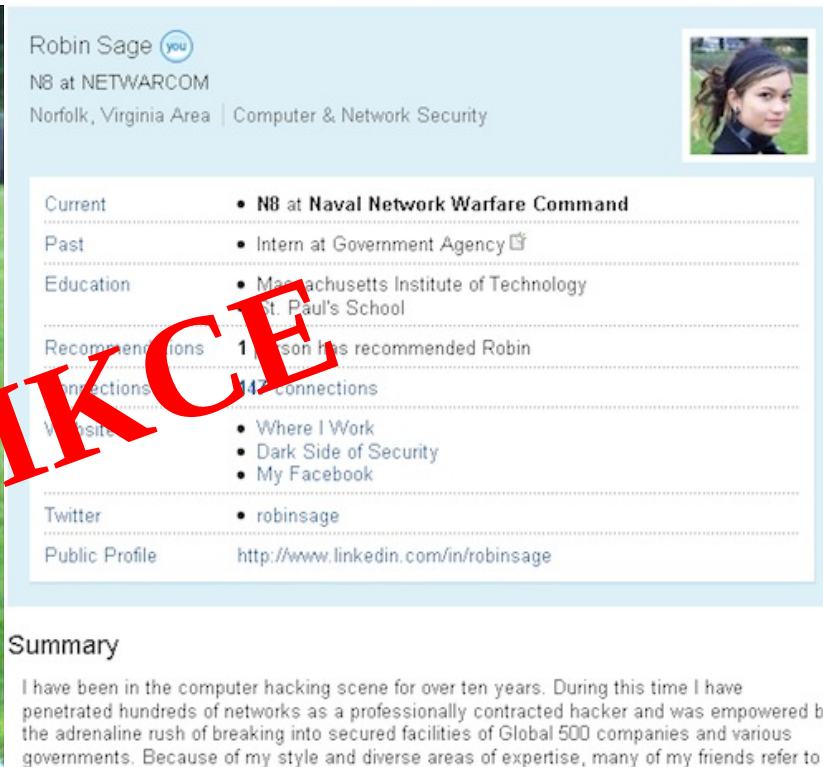
**PLEASE ROB ME .com**

- Fotografie
  - GeoTag -> EXIF
- Wifi síť - SSID



## Robin Sage experiment

- Specialistka na bezpečnost, 25 let
- Stovky přátel během několika měsíců  
Bezpečnostní oddělení firem, vládní a armádní složky...



**Robin Sage** (you)

N8 at NETWARCOM

Norfolk, Virginia Area | Computer & Network Security

**Current**

- N8 at Naval Network Warfare Command

**Past**

- Intern at Government Agency

**Education**

- Massachusetts Institute of Technology
- St. Paul's School

**Recommendations** 1 person has recommended Robin

**Connections** 142 connections

**Website**

- Where I Work
- Dark Side of Security
- My Facebook

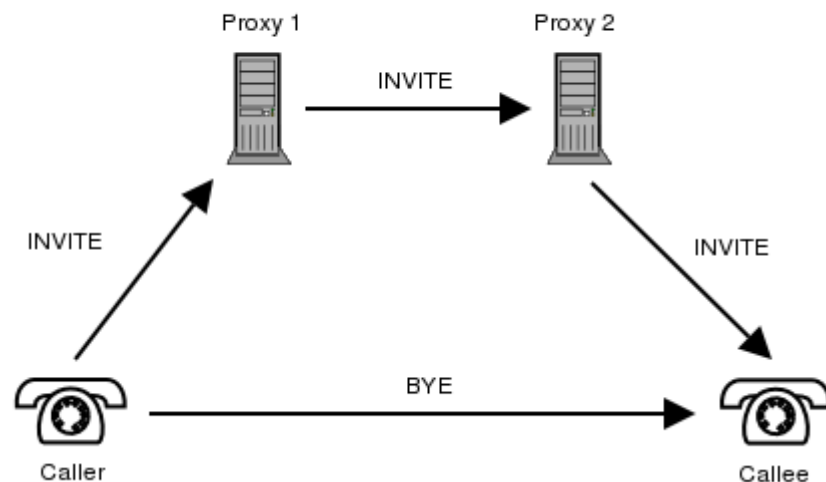
**Twitter** • robinsage

**Public Profile** <http://www.linkedin.com/in/robinsage>

**Summary**

I have been in the computer hacking scene for over ten years. During this time I have penetrated hundreds of networks as a professionally contracted hacker and was empowered by the adrenaline rush of breaking into secured facilities of Global 500 companies and various governments. Because of my style and diverse areas of expertise, many of my friends refer to me as the real life Abby Scuito of NCIS.

- Spear phishing
- Krádež identity
- Man-in-the-Middle



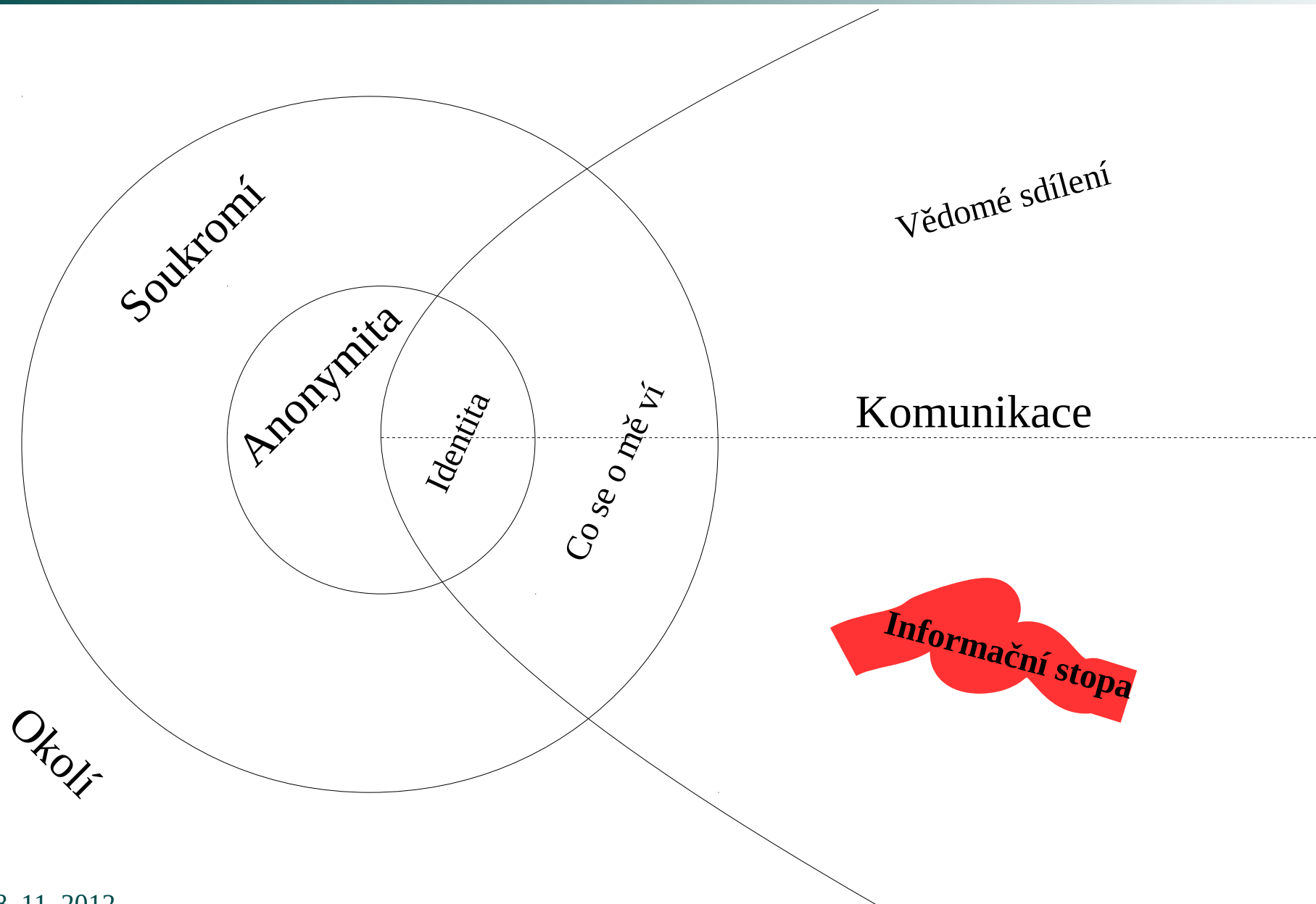
Hello,

I'm sorry for this odd request because it might get to you too urgent, but due to the situation of things right now, I'm stranded in London with my family right now, we came down here on a train that was robbed, worst part is that wallet, cash credit cards and my passport was stolen at GUN POINT, It's such a crazy experience for me. I need help flying back home, the authorities are not being 100% helpful. The good thing is we still have our passport but don't have the money to get my flight ticket back home and some bills sent home. We need you to loan me some money, will refund you as soon as I get home, I promise.

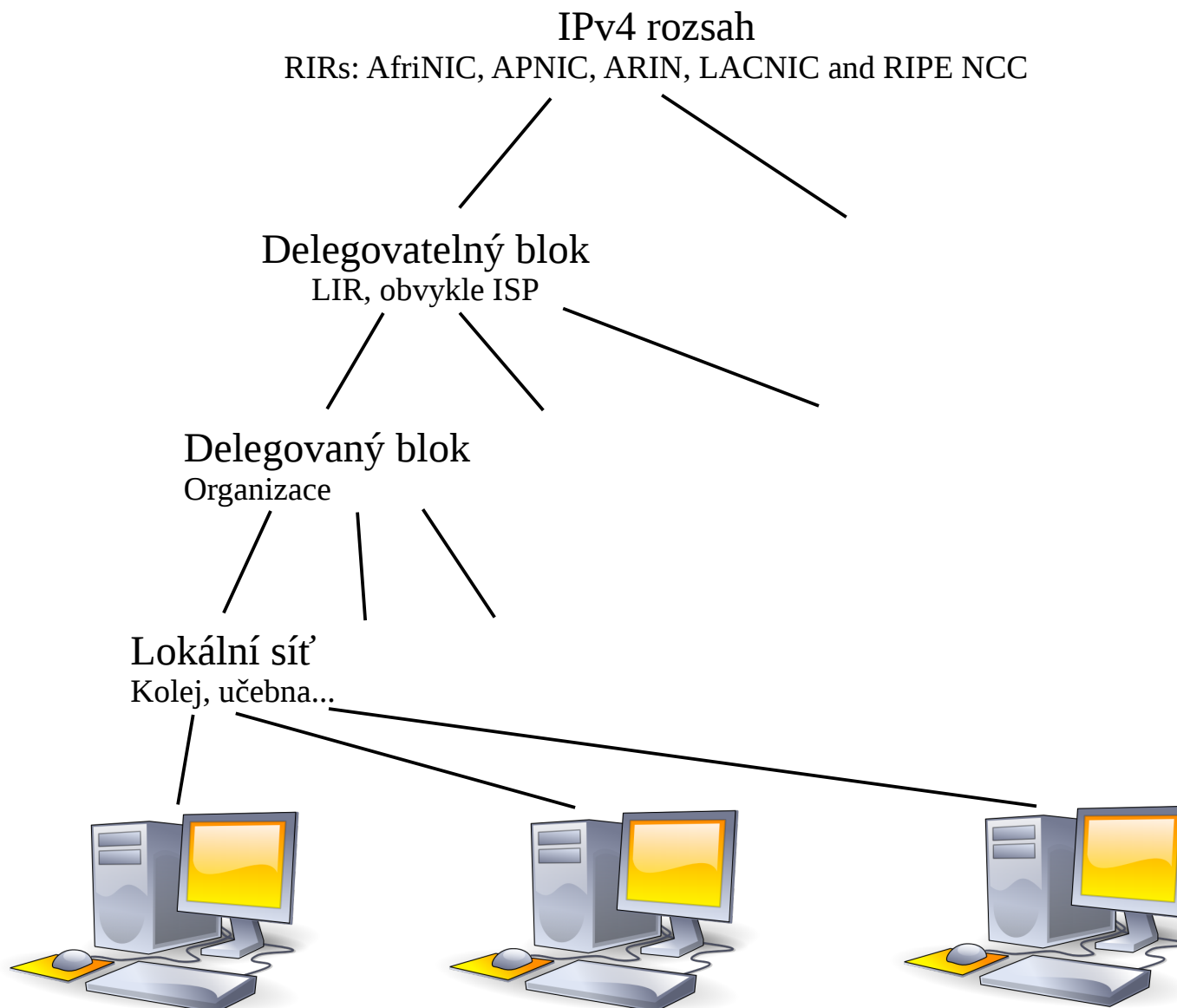
Thanks

Martha & Thomas Norman-Smith

# Informační stopa







RIPE  
↓  
CESNET  
↓  
MUNI  
↓  
Kolej  
↓  
Uživatel

- Přidělování IP adres
  - Na základě HW adresy (MAC) – žádost uživatele
  - Na základě elektronické identity (login +heslo)
- Bezdrátové sítě
  - Možnost určení polohy (triangulace)
  - Pozor na provoz vlastního AP!
- Vazba *IP adresa – čas – uživatel*
  - Lokální správce ví přesně, komu a kdy bylo IP přiděleno
  - Používaná IP adresa není anonymní!

- Co o nás napíše jiní
  - V diskusích, na sociálních sítích
  - Na firemních a školních webech
- Zpětné odkazy
- Interview, videa
- Fotografie
  - Označené osoby
  - EXIF
  - Identifikovatelné objekty



Na této fotce označen:  
[Pavel Kácha](#)

Přidáno 20 leden  
· [To se mi líbí](#)   
· [Přidat komentář](#)



Return-Path: johann@cesnet.cz  
X-Original-To: ph@cesnet.cz  
Delivered-To: ph@office2.cesnet.cz  
Received: from [195.113.xxx.yyy] (eduroam-XXX.cesnet.cz [195.113.xxx.yyy])  
by viden.cesnet.cz (Postfix) with ESMTP id 01567D800D1  
for <ph@cesnet.cz>; Mon, 1 Dec 2008 15:58:41 +0100 (CET)  
Subject: Re: Pozdravy z Vidne  
From: Johann Strauss <johann.strauss@cesnet.cz>  
To: Pavel Kácha <ph@cesnet.cz>  
In-Reply-To: <20081201142058.GB1602@cesnet.cz>  
Date: Mon, 01 Dec 2008 15:58:44 +0100  
Message-Id: <1223453524.3834.24.camel@eduroam-221.cesnet.cz>  
Mime-Version: 1.0  
X-Mailer: Evolution 2.12.3 (2.12.3-5.fc8)

- Skutečný odesílatel
- Cesta přes servery
- Zdrojové jméno počítače
- Platforma
- Mailový klient, včetně přesné verze

```
connection: keep-alive
accept-language: cs,en;q=0.7,en-us;q=0.3
content-length: 0
accept-encoding: gzip,deflate
referer: http://www.google.com/search?q=cesnet&ie=UTF-8&oe=UTF-8
host: www.cesnet.cz
accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
accept-charset: windows-1250,utf-8;q=0.7,*;q=0.7
keep-alive: 300
user-agent: Mozilla/5.0 (X11; U; Linux i686; cs-CZ; rv:1.9.0.4)
 Gecko/2008112309 Icedweasel/3.0.3 (Debian-3.0.3-3)

cookie: UID=ph; SESSION_ID=AF347DC667.33985
```

- Referer – stránka, ze které přicházím
- Prohlížeč včetně přesné verze
- Platforma včetně přesné verze
- Cookie – identifikace uživatele nezávisle na IP adrese (personalizace, sledování)

<http://browserspy.dk> <http://panopticlick.eff.org> <http://samy.pl/evercookie/>

- Cookie, Flash Cookie, Silverlight Storage, IE UserData, HTML5 Storage, Cache, ETags, historie...

*samy.pl/evercookie*

- UserAgent, HTTP\_ACCEPT, nainstalované pluginy, fonty, časová zóna, rozlišení, cookies, JS vlastnosti

*panopticlick.eff.org*

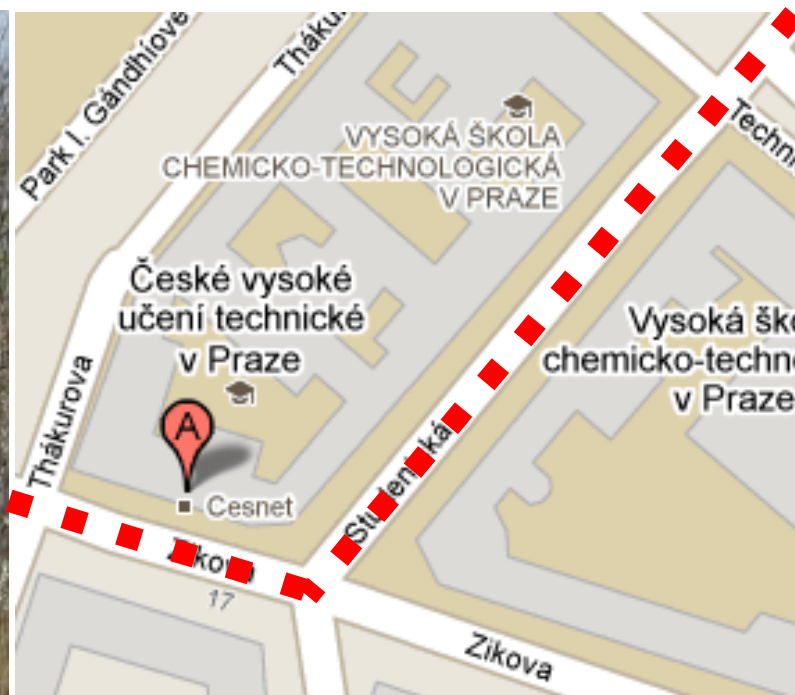
- Zkuste si sami

*browserspy.dk*



- Ve většině sítí je stahovaný obsah automaticky nabízen
  - Někdy lze v klientech omezit (pozor na nastavení po instalaci)
  - U některých je to nedílná vlastnost protokolu (BitTorrent)
- Po připojení do P2P sítě
  - Informace o mně (a mé nabídce) se šíří sítí
  - Vidí je každý, kdo o ně má zájem ...  
... tedy i vlastníci autorských práv!
  - Velké filmové společnosti jsou velmi aktivní





Wardriving ve velkém...



... a v menším





Karty

Vstupní tokeny

Auto zámky

Sledování zboží

Budoucnost:  
pasy, kreditní karty



## OPENCARD

Po zveřejněných  
informacích  
vnímám tuto  
kارتu jako:

**18**  
nemá  
názor

**17**  
důvěryhodnou

opencard

názory  
české  
veřejnosti  
v %

**65**  
nedůvěryhodnou

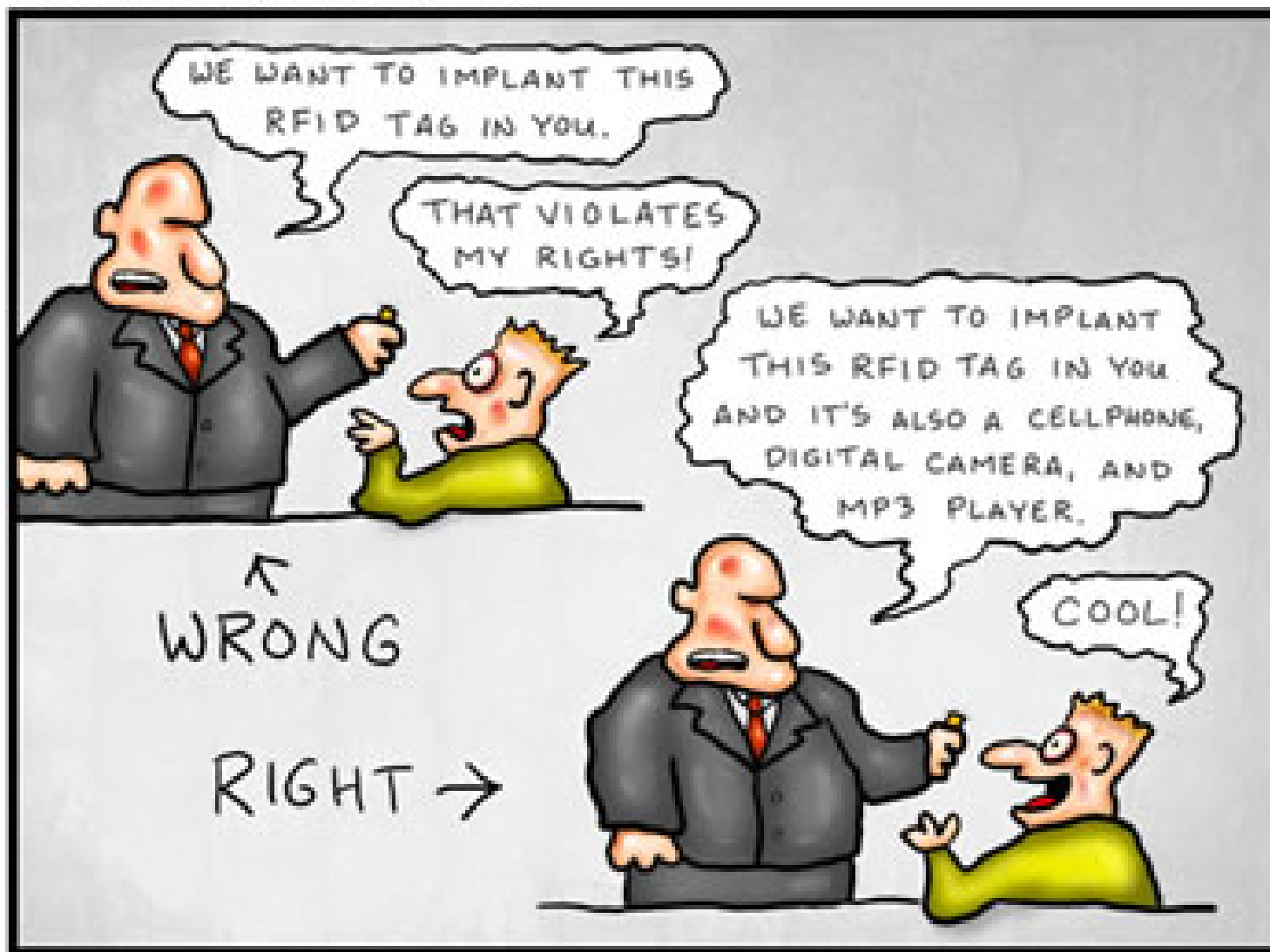
zdroj: SANEP

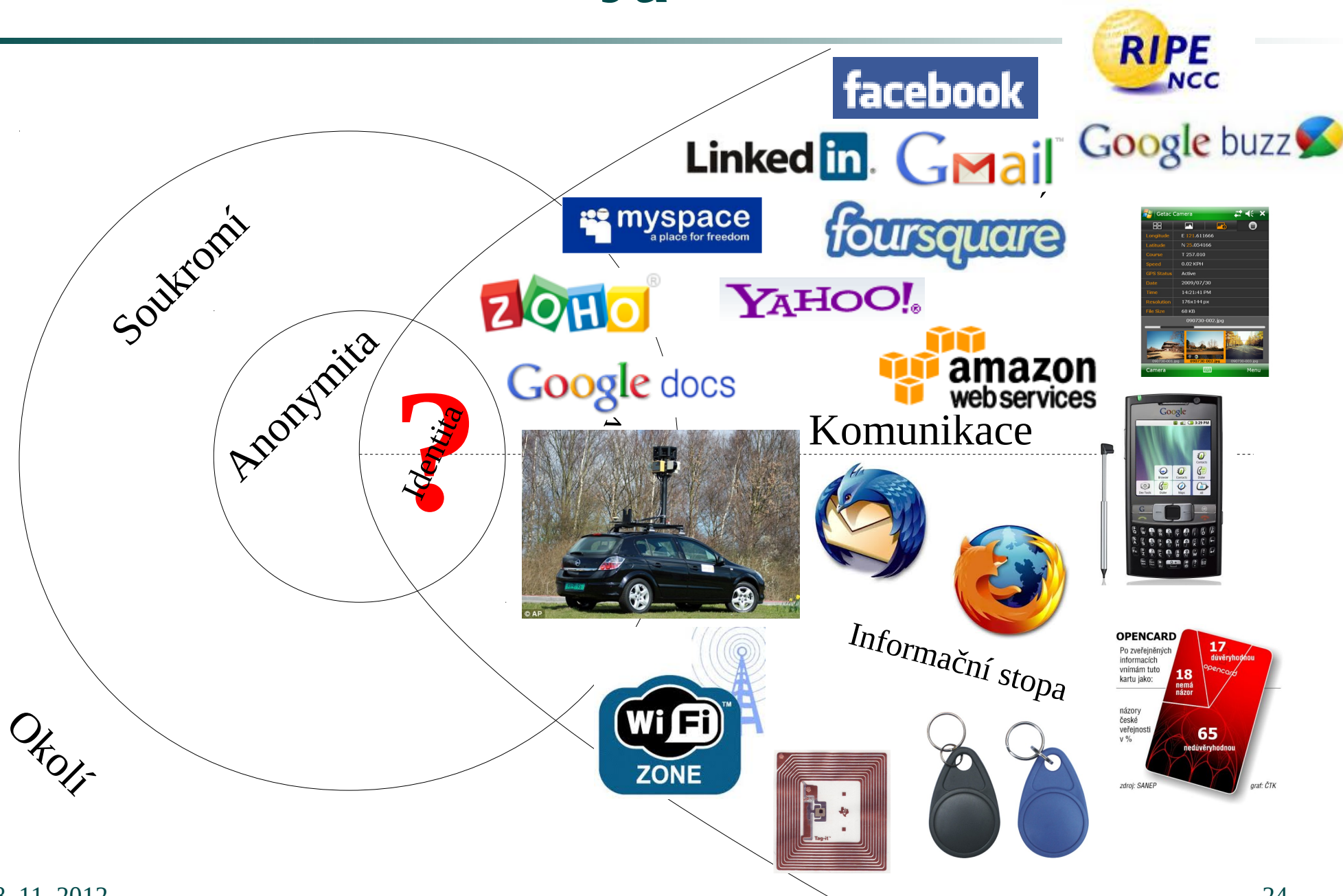
graf: ČTK

# A nemůžeme si za to sami..?

## DOCTOR FUN

16 Jan 2006





# Děkuji za pozornost.

---