Social Networking Security

Online Social Networking (OSN)

- Online Web services enabling people to connect with each other, share information
  - Common friends, interests, personal info, …
  - Post photos, videos, etc. for others to see
  - Communicate via email, instant message, etc.
- Major OSN services: Facebook, Twitter, MySpace, LinkedIn, etc.

OSN Popularity

- Over 2.2 billion Facebook users worldwide
- Over 330 million Twitter users; over 100 million users connected daily
- Over 460 million LinkedIn members in over 200 countries
- Capitalization Facebook 391 Billion US$ (Italian stock market abut 559 Billion Euro)

Benefits of OSN Communication

- Vast majority of college students use OSNs
  - Organizations want to market products, services, etc. to this demographic
  - OSNs can help them reach these potential buyers
- OSNs provide communal forum for expression (self, group, mass), collaboration, etc.
  - Connect with old friends, find new friends and connect
  - Play games with friends, e.g., Mafia Wars, Scrabulous
  - Commerce in “virtual items”
- But using OSNs poses security issues for orgs as well as individuals

Outline

- **Threats and Attacks: Malware**
- Use of personal information
- Defense measures
- Threats and attcaks: deanonymization

OSN Security Threats/Attacks

- Malware distribution
- Cyber harassment, stalking, etc.
- Information “shelf life” in cyberspace
- Privacy issues:
  - Information about person posted by him/herself, others
  - Information about people collected by OSNs
- Information posted on OSNs impacts unemployment, insurance, etc.
- Organizations’ concerns: brand, laws, regulations

URL Shorteners

- bit.ly, TinyUrl, ReadThisURL, NotLong
- Hides the true destination URL – hard to tell where you're going until you click!

`http://www.evil.com/badsite?%20infect-your-pc.html`

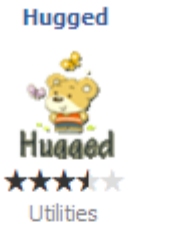
is now

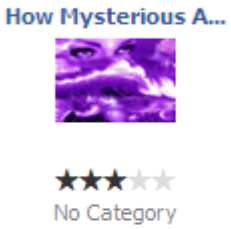
`http://bit.ly/aaI9KV`

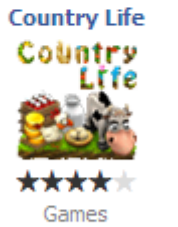
OSN Malware Distribution

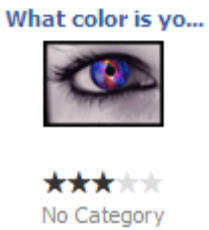
- Best-known example: Koobface [9–10]
  - Worm masquerading as Adobe Flash Player update
  - Starting in 2009, OSN users enticed to watch “funny video”, then conned into “updating” Flash
  - Koobface connected infected computers to botnet, served machines ads for fake antivirus software
  - Estimated 400,000–800,000 bots in 2010
  - Facebook outed gang behind Koobface in Jan. 2012, bot server shut down
- Other third-party apps on OSNs like Facebook may contain malware (if not vetted)
- Not to mention hoaxes, “chain letters,” and other cons

OSN 3rd Party Applications



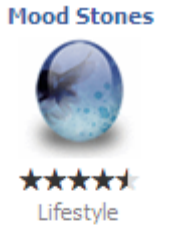


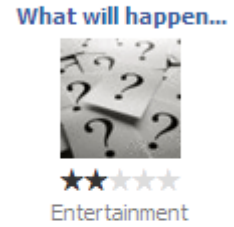


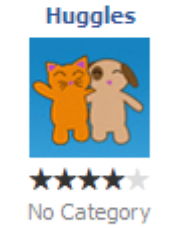


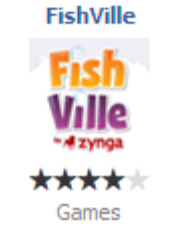
- Games, quizzes, "cute" stuff
- Untested by Facebook – anyone can write one…
- No Terms and Conditions – either allow or deny
- Installation gives developers rights to look at your profile and overrides your privacy settings!

There's a sucker born every minute.
–P.T. Barnum









Outline

- Threats and Attacks: Malware
- **Use of personal information**
- Defense measures
- Threats and attcaks: deanonymization

OSN Stalking, Harassment, etc.

- Bullies, stalkers, etc. harass people via OSNs
  - High-profile example: Megan Meier's suicide [11–12]
    - 13-year old Meier killed herself after chatting on MySpace with a 16-year-old boy who made degrading remarks
    - The "boy" was a fake account set up by Lori Drew, mother of Meier's ex-friend
    - Drew found guilty of violating Computer Fraud and Abuse Act in 2008; acquitted in 2009
    - Most U.S. states have since criminalized cyber harassment, stalking, etc.
  - OSNs (and their members) have played similar roles in mistreating people

How much information are you publicly sharing?

- Facebook users sometimes unknowingly share personal information with complete strangers. For example, phone numbers, personal and work email address, pictures and the user's location information are readily available.
- All of this information could be useful when combined with social engineering techniques to aid in identity theft or the compromising of sensitive information.

Social Networks and Social Engineering

- Malicious actors are targeting Social network users to gain information to be used in phishing and other attacks
- Users are often not aware of the amount of information that is unwittingly shared in social networking sites
- Social Engineering is the often the precursor to targeted APT attacks on companies

Facebook Groups and Apps

- Specifically, Facebook groups can be used to social engineer private information from users
- Games and other Applications in Facebook are often infected with malware and/or infected links that compromise the security of the user and all of their connected friends
- Awareness and careful vetting of all connected friends is critical to securing the Facebook experience

Social Media Abuse

- As in any large scale social gathering, whether physical or virtual, there are always abusers and criminals involved.
- Facebook allows criminals to conceal their identity by creating fake accounts in order to carry out malicious activities anonymously.
- Many crimes have been solved using Facebook as a social networking source

What is Phishing?

Common attack performed on Facebook users.

Phishing websites are malicious, "imitation websites" that look practically identical to the original website. The main purpose of these websites are to steal confidential information such as usernames and passwords or financial information.

Website has to look authentic

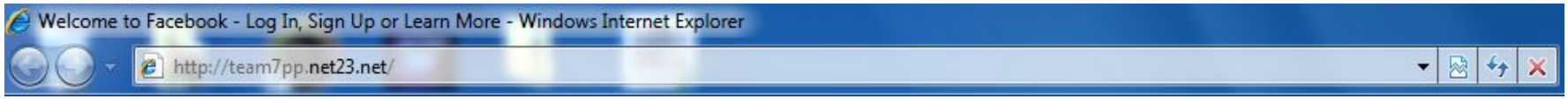
- The phishing website has to look authentic for the user to be tricked into entering their login credentials.
- There are ways to identify if you are on a legitimate website, but many Facebook users will fall for this trick.

Which is the real Facebook?

Is this the real Facebook?

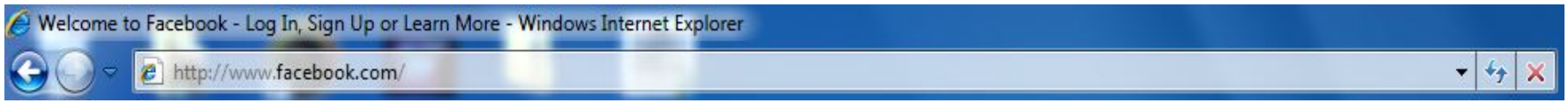
How can you tell which is real?

Phishing Website



Always check the address bar of the website you are on!

Authentic Website



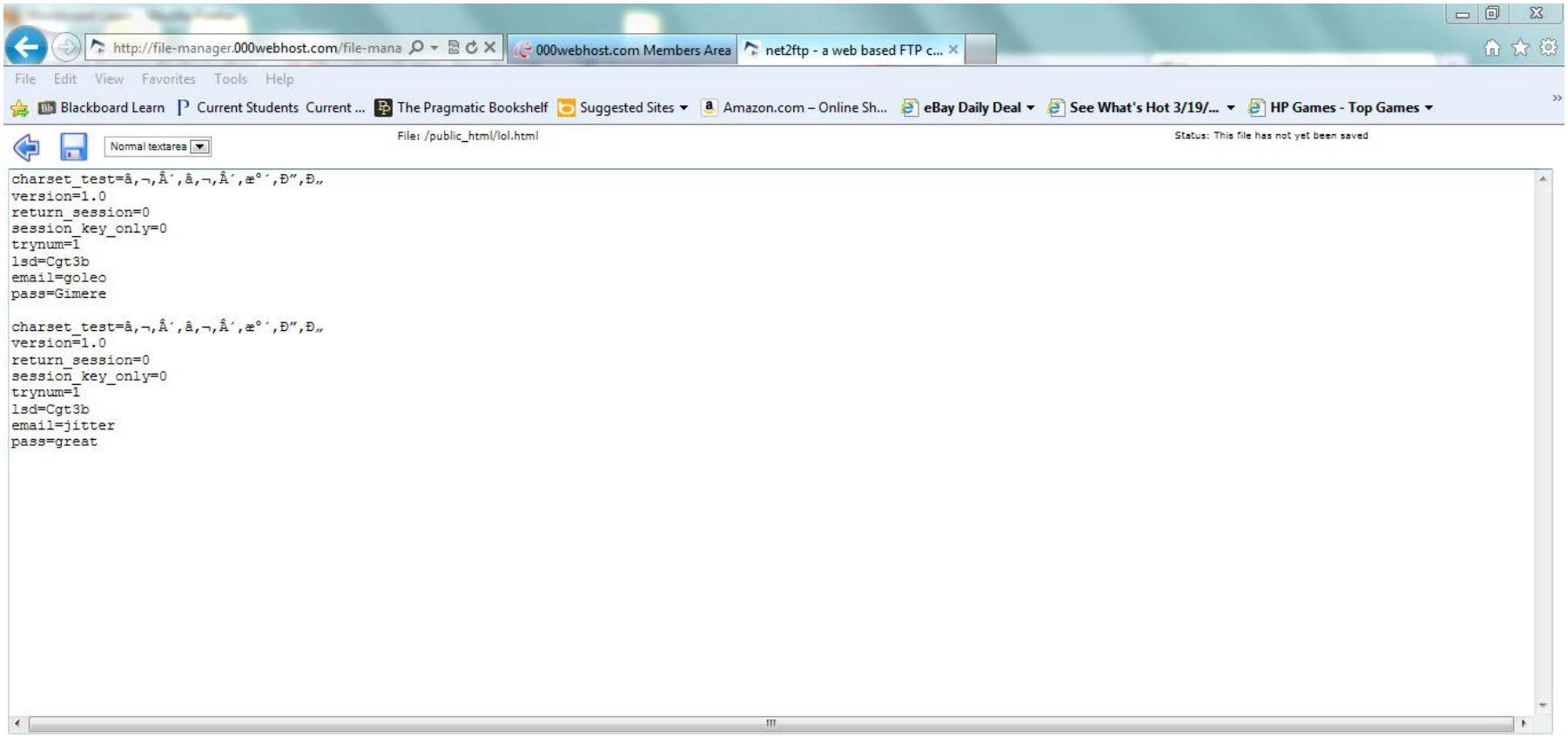
Establish Trust

- As with any type of social engineering attack, the attacker must convince the victim that you are trustworthy. This can be done in many ways.
- For example, the attacker may have made a fake Facebook account to get access to your friends list. From there, the attacker can create a fake email address that impersonates the name of one of their friends. For example, Thomas.Hardy@gmail.com. Or the attacker can pose to be a leader of a fan group for a sports team listed under their favorite teams section.
- This is how attackers can mine information on a specific user in order to craft a unique attack.

Retrieve Login Information

- Once the victim types in their account information, the hacker now has the login credentials to the user's Facebook account. Once the user attempted to login to the fake webpage, their login credentials got sent to a file on the hacker's server called "lol.html" in this case.
- We can now login as the victim and spread the attack to their friends.

User’s login credentials

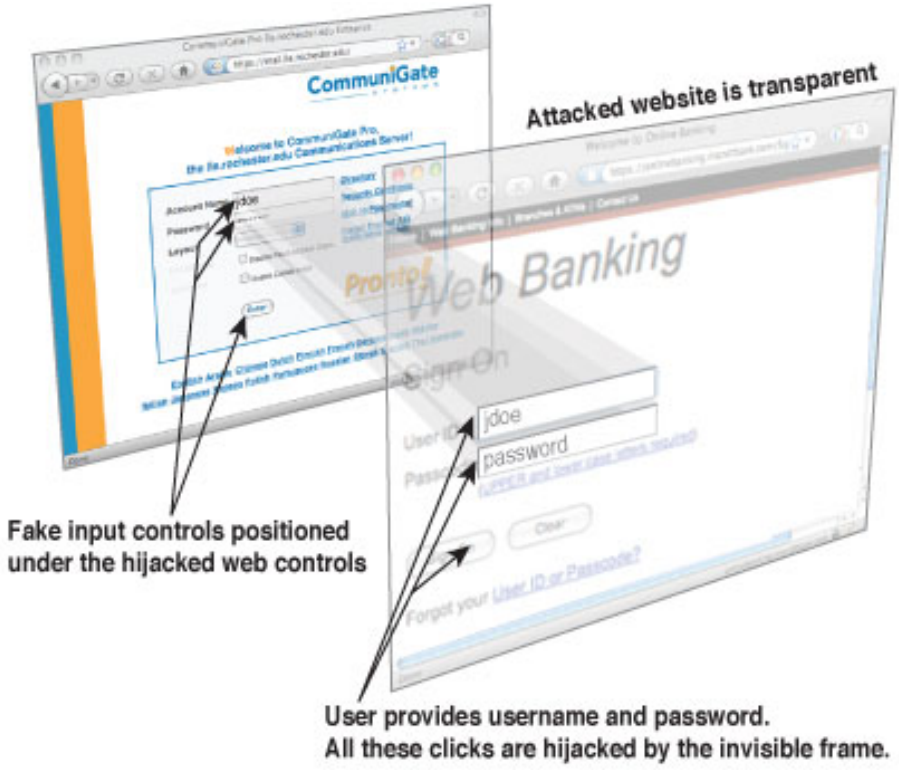


What is “Clickjacking”

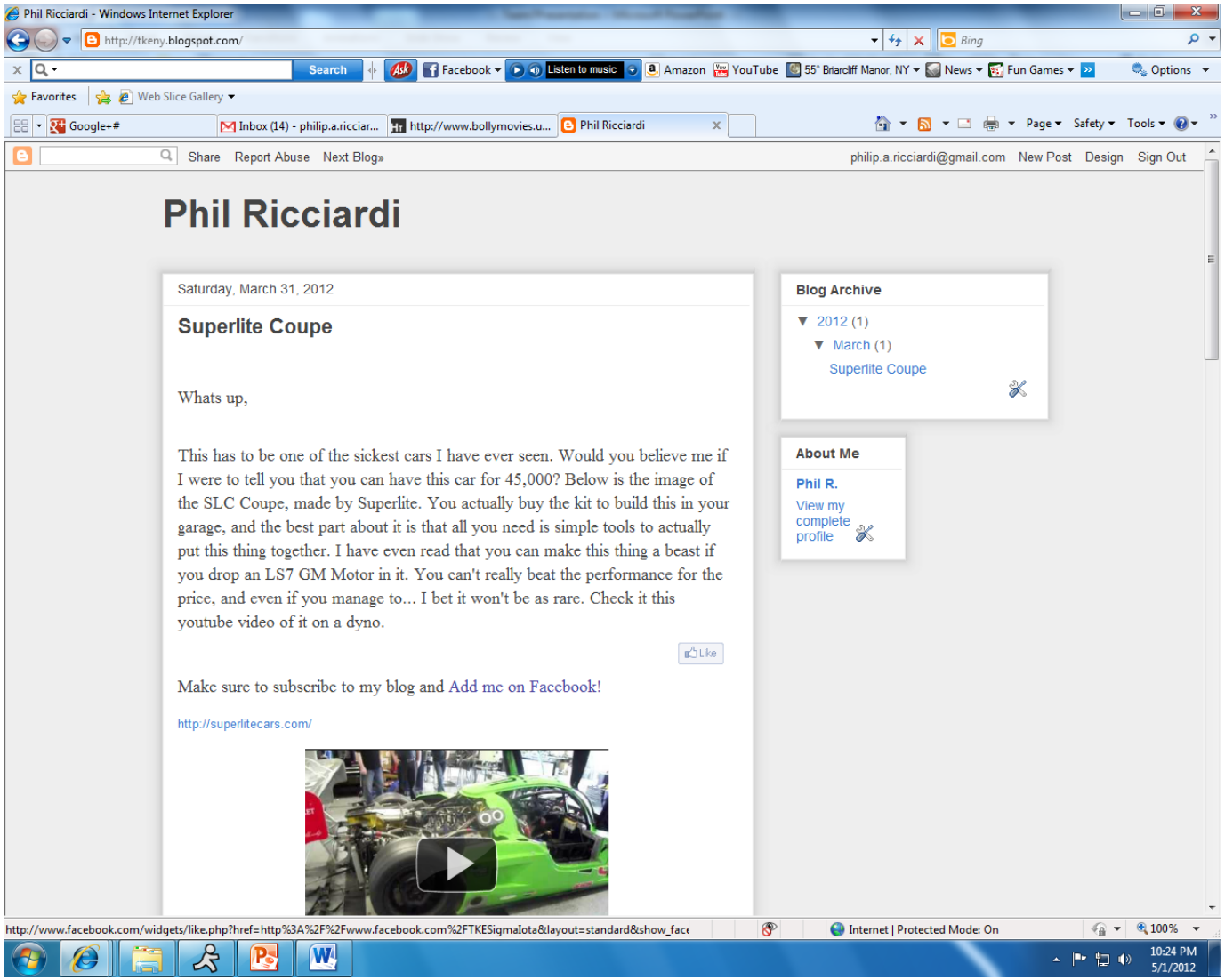
- Clickjacking tricks users into clicking on a specific portion of a webpage that performs an action other than what they are intending

How a clickjacking attack works?

- Utilizes JavaScript technology to create a transparent frame that hovers above the website the user actually sees.



Clickjacking Blog



Clickjacking is an easy way to attract attention to a Facebook business page or fan page.

Clickjacking Defenses

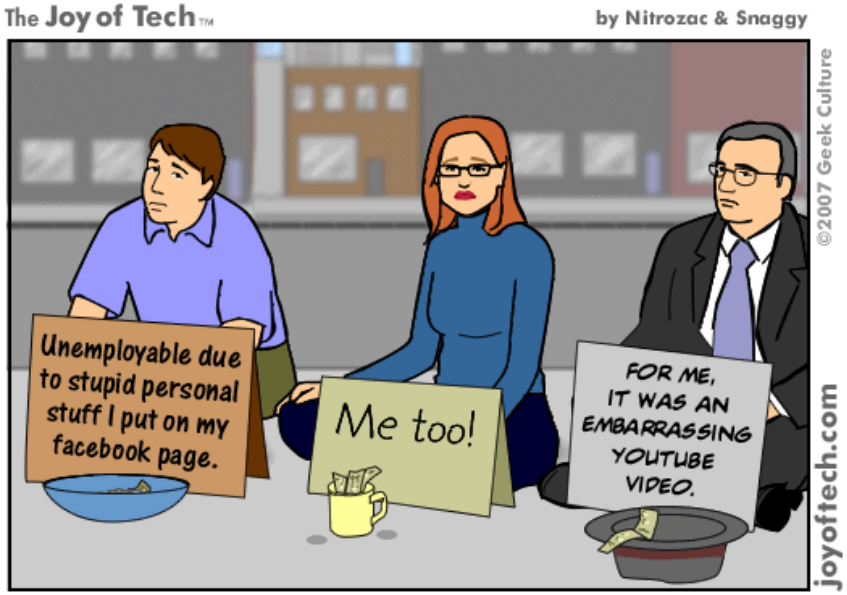
- Clickjacking attacks are difficult to identify and prevent.
- Staying logged into online accounts such as amazon.com and Facebook while surfing the internet puts you at a much greater risk.

Final Thoughts

- Phishing and clickjacking attacks are a very real threat to users on the Facebook network. Many attacks like these are carried out everyday. Our personal information is at risk.
- Facebook is only as secure as the user is smart. It is up to the user to follow safe practices when using social networking websites. Some of the attacks described are nearly impossible to avoid. Facebook users need to be properly trained on how to identify these types of attacks.

OSN Information "Shelf Life"

- Common sense: it's very difficult to delete information after it's been posted online
- Indiscreet information can adversely affect college admissions, employment, insurance, etc.
- Twitter gave its entire archive to Library of Congress in 2010

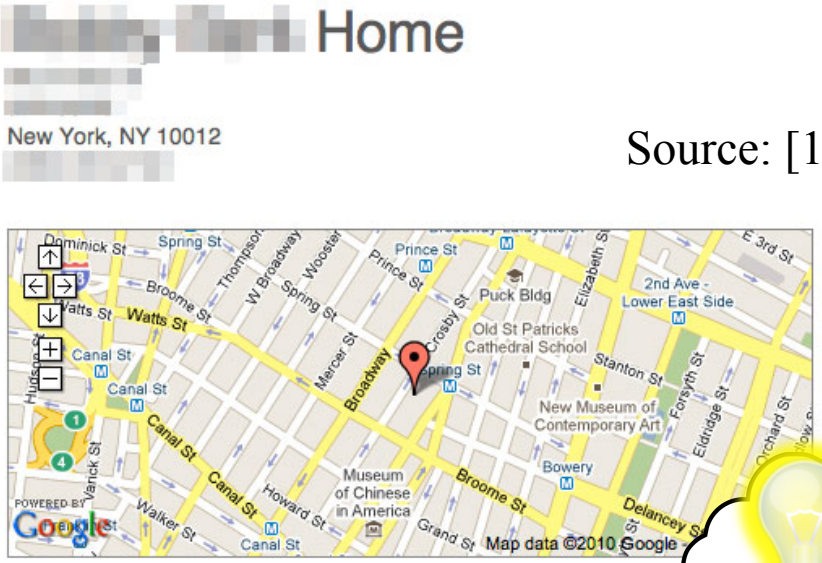


Signs of the social networking times.

Originally posted in [2].

OSN Information Privacy (1)

- Information posted on OSNs is generally public
  - Unless you set privacy settings appropriately
  - "I'll be on vacation" post plus geolocation invites burglars, i.e., "Please Rob Me" [14]
- Indiscreet posts can lead to nasty consequences



Source: [14]

Map from [14]; other images public domain

OSN Information Privacy (2)

- Employers, insurers, college admissions officers, et al. already screen applicants using OSNs
- Recent report from Novarica, research consultancy for finance and insurance industries:

"We can now collect information on buying behaviors, geospatial and location information, social media and Internet usage, and more…Our electronic trails have been digitized, formatted, standardized, analyzed and modeled, and are up for sale. As intimidating as this may sound to the individual, it is a great opportunity for businesses to use this data."

OSN Information Privacy (3)

- Posts that got people fired:
  - Connor Riley: “Cisco just offered me a job! Now I have to weigh the utility of a [big] paycheck against the daily commute to San Jose and hating the work.”
  - Tania Dickinson: compared her job at New Zealand development agency to “expensive paperweight”
  - Virgin Atlantic flight attendants who mentioned engines replaced 4 times/year, cabins with cockroaches

OSN Information Privacy (4)

- OSNs don't exactly safeguard posted info…

Facebook

Facebook and Other Social Media Networks Found Sending Data to Advertisers

21. MAY, 2010 4 COMMENTS AUTHOR: TIM ROENICKE

perpetual,
right to us
remove, r
known or
indirectly
ideas, con
without ar
parties. A

works and distribute (through multiple tiers), any User Content you (i) Post on or in connection with the Facebook Service or the promotion thereof subject only to your privacy settings or (ii) enable a user to Post, including by offering a Share Link on your website and (b) to use your name, likeness and image for any purpose, including commercial or advertising, each of (a) and (b) on or in connection with the Facebook Service or the promotion thereof. You may remove your User Content from the Site at any time. If you choose to remove your User Content, the license granted above will automatically expire, however you acknowledge that the Company may retain archived copies of your User Content."

OSN Information Privacy (4)

- OSNs don't exactly safeguard posted info…

Facebook

One of the few coherent messages to emerge from the US Senate's bumbling interrogation of Mark Zuckerberg was a touching desire that Facebook's user agreement should be comprehensible to humans. Or, as Sen. J.Kennedy of Louisiana put it: "Here's what everyone's been trying to tell you today – and I say it gently – your user agreement sucks. The purpose of a user agreement is to cover Facebook's rear end, not inform users of their rights."

"I would imagine probably most people do not read the whole thing," Zuckerberg replied. "But everyone has the opportunity to and consents to it." Senator Kennedy was unimpressed. "I'm going to suggest you go home and rewrite it," he replied, "and tell your $1,200 dollar an hour lawyer you want it written in English, not Swahili, **so the average American user can understand."**

OSN Information Privacy (4)

- OSNs don't exactly safeguard posted info…

> Facebook
> Specifically, when you share, post, or upload content that is covered by intellectual property rights (like photos or videos) on or in connection with our Products, you grant us a non-exclusive, transferable, sub-licensable, royalty-free, and worldwide license to host, use, distribute, modify, run, copy, publicly perform or display, translate, and create derivative works of your content (consistent with your privacy and application settings). This means, for example, that if you share a photo on Facebook, you give us permission to store, copy, and share it with others (again, consistent with your settings) such as service providers that support our service or other Facebook Products you use.
> You can end this license any time by deleting your content or account. You should know that, for technical reasons, content you delete may persist for a limited period of time in backup copies (though it will not be visible to other users). In addition, content you delete may continue to appear if you have shared it with others and they have not deleted it.

Key aspects: social media

consent and data use are covered by the terms and conditions and privacy notices of each platform

- Example: it is acceptable to take an email address from social media, hold or use it in any marketing activity, if you can justify doing so via legal grounds and provided you comply with the GDPR principles.
- You can continue to message via the social media platform where you have made a connection (liked or followed), but you can’t move the communication to any other marketing channel unless you can satisfy those legal grounds and comply with the data protection principles.

Key aspects: social media

Key definitions

- **Controller**: the company/person who decides how and why personal data is processed
- **Data subject**: an identifiable living individual
- **Personal data**: any information relating to a data subject
- **Processing**: doing anything in relation to personal data
- **Processor**: the company/person who processes personal data on behalf of the controller
- **Recipient**: a company/person to which personal data is disclosed

Key aspects: social media

LinkedIn is a data controller and has responsibility for ensuring compliance with GDPR; it is certified under the EU-US privacy shield.

- GDPR will, however, have some effects on their products such as LinkedIn Marketing Solutions, Sales Solutions and Talent Solutions.
- Now all members will have the option of opting out of allowing use of their demographic data in ad targeting. Members will control this from a new advertising settings page

Key aspects: social media

Facebook: in most cases is a data controller.

- There are some key instances, in which Facebook may also serve as a data processor.
- Example, the case if you use Custom Audiences – when you upload a list of customers from your database to target with Facebook ads.
- Whenever you create a Facebook ad you are asked to accept their terms and conditions; these are due to change before 25th May to comply with GDPR.

Key aspects: social media

Twitter is primarily a data controller.

- As with LinkedIn, and Facebook, when you upload your own data to create a Tailored Audience for advertising, Twitter becomes a data processor. You are the data controller and are responsible for ensuring you have legal grounds to process the data before transferring it to Twitter for processing.

Key aspects: social media advertising

- when a company is providing personal data to any advertising platform they will need to have the right to do so under the GDPR.
- When advertising on social media you will need to ensure there is a suitable disclaimer and link to a privacy policy on any form you use when capturing data.

social media advertising: before GDPR

When advertising on social media

- No pre-ticked opt-in boxes for consent.
- If you're collecting data in exchange for content such as downloads consent for marketing communication needs to be explicit and opt-in
- If you are outsourcing social media management, then you need a data processing agreement: there must be a written contract when one business processes personal data on behalf of another business.

Key aspects: social media advertising

If you are outsourcing social media management, then there must be a written contract; key aspects

- the length of time of the processing
- the type(s) of personal data
- obligations and rights of the data controller
- all of the data processor's personnel who access the data is subject to confidentiality obligations
- the data processor will comply with the GDPR regarding security measures and encryption
- the data processor must assist the data controller in dealing with requests from data subjects, dealing with data breaches and conducting impact assessments

Facebook‘s privacy policy,

Patent Facebook US20180012146A1 –

•Patent for “**sentiment polarity for users of a social networking system**”. It’s about **how to infer the sentiments in a web user by viewing a web page**.

•“The sentiment polarity of the user is inferred based on received information about an interaction between the user and the page (eg like, report etc), and may be based on analysis of a topic extracted from text on the page. The system infers a positive or negative sentiment polarity of the user toward the content of the page, and that sentiment polarity then may be associated with any second or subsequent interaction from the user related to the page content.” This is surveillance capitalism in action.

Facebook‘s privacy policy,

A controversial experiment

The "one week study in January of 2012”: over 600,000 users were randomly selected to unknowingly partake in a study to determine the effect of "emotional alteration" by Facebook posts.

Apart from the ethical issue of conducting such a study with human emotion in the first place, this is just one of the means in which data outsourcing has been used as a breach of privacy without user disclosure

Facebook‘s privacy policy, revisited (before 2017)

“Facebook also collects information about you from other sources, such as newspapers and instant messaging services. This information is gathered regardless of your use of the Web Site.”

- 85% believe that is *not* the case

“We use the information about you that we have collected from other sources to supplement your profile unless you specify in your privacy settings that you do not want this to be done.”

- 87% believe that is *not* the case

“In connection with these offerings and business operations, our service providers may have access to your personal information for use in connection with these business activities.”

- 60% believe that is *not* the case

- Control: perusal of privacy policy does *not* improve awareness

Awareness of users

Facebook users have limited awareness on privacy issues.

- The most common strategy for privacy protection—decreasing profile visibility through restricting access to friends
- This could be a very weak mechanism. In fact many users are accepting people as "friends" that they have only heard of through other or do not know at all and, therefore, most have very large groups of "friends" that have access to personal information and pictures.

Therefore

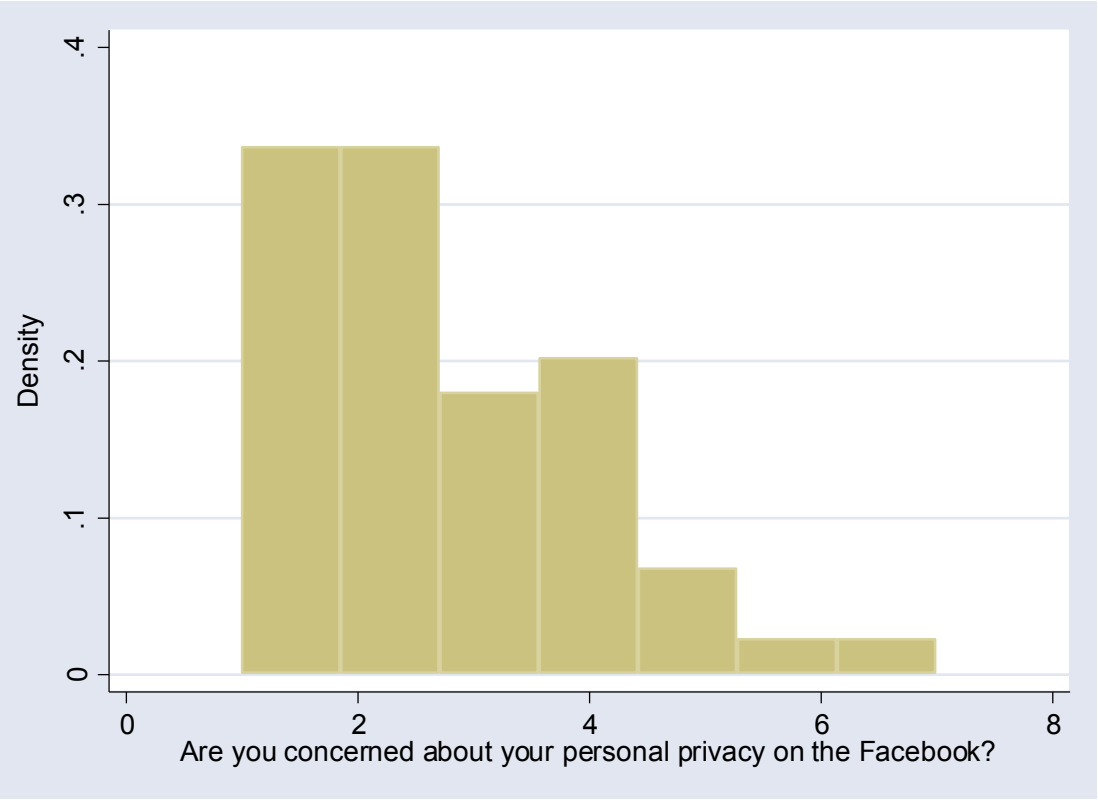
- social network privacy does not merely exist within the realm of privacy settings, but privacy control is within the hands of the user
- more education about privacy on Facebook would be beneficial to the majority of the Facebook user population.

Privacy concerns

- 69% believe that the information *other* Facebook users reveal may create privacy risks for those users
- But:

Conclusion:

No rational behaviour



Information revelation

- Reasons to provide more personal information (in order of importance):
  1. No factor in particular, it's just fun
  2. No factor in particular, but the amount of information I reveal is necessary to me and other users to benefit from the *FaceBook*
  3. No factor in particular, rather I am following the norms and habits common on the site
  4. Quite simply, expressing myself and defining my online persona
  5. Showing more information about me to "advertise" myself

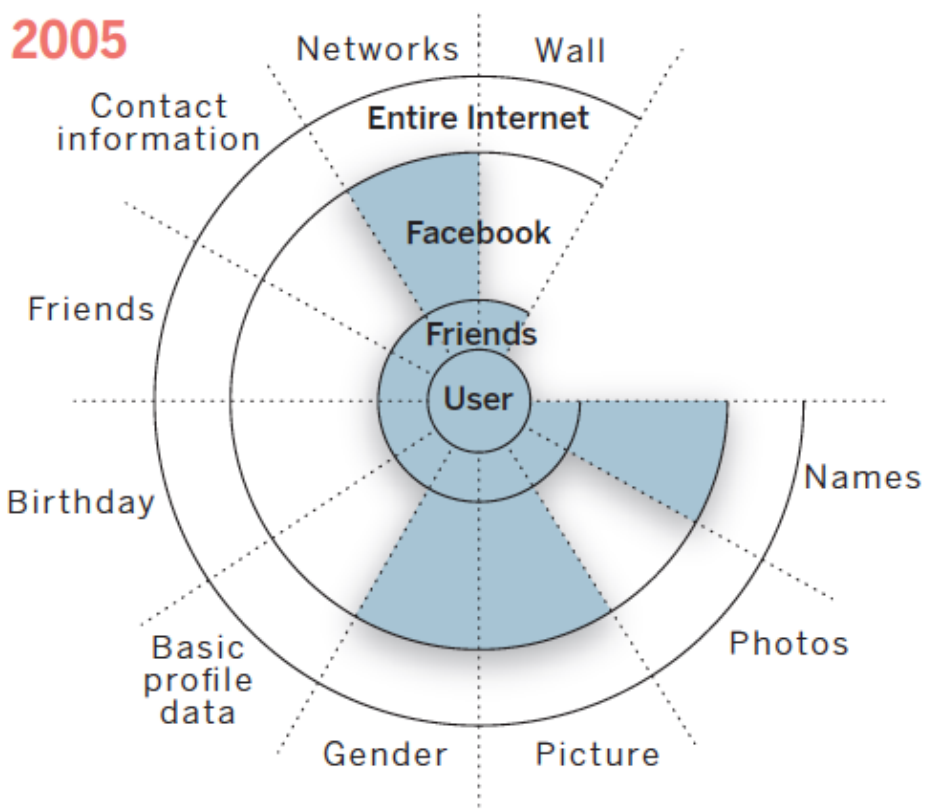
  …..

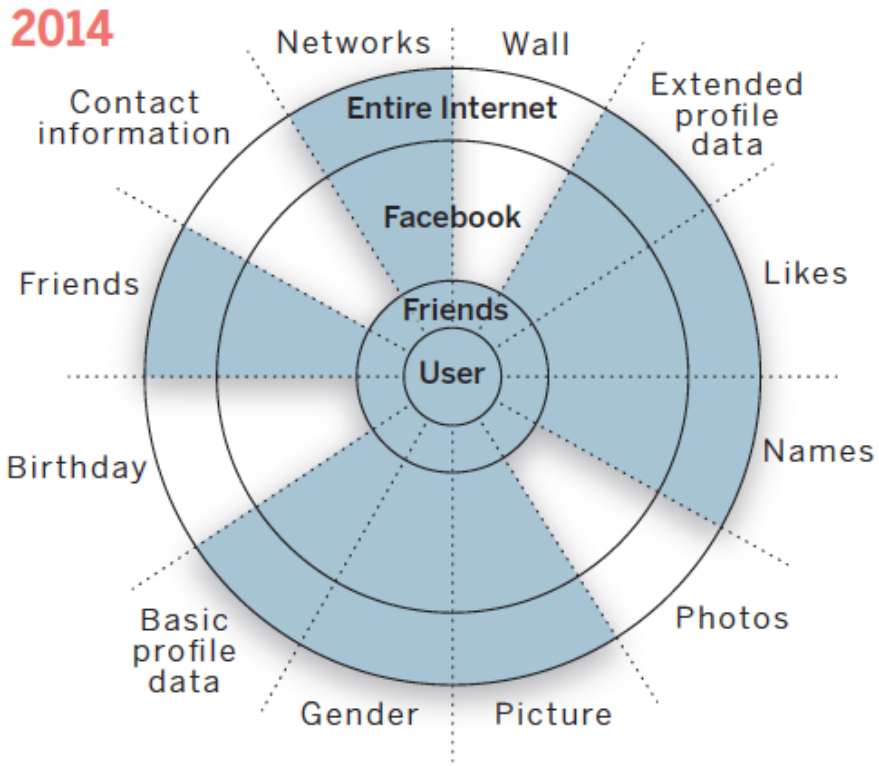
  – Getting more potential dates

Default visibility settings in social media

VISIBLE

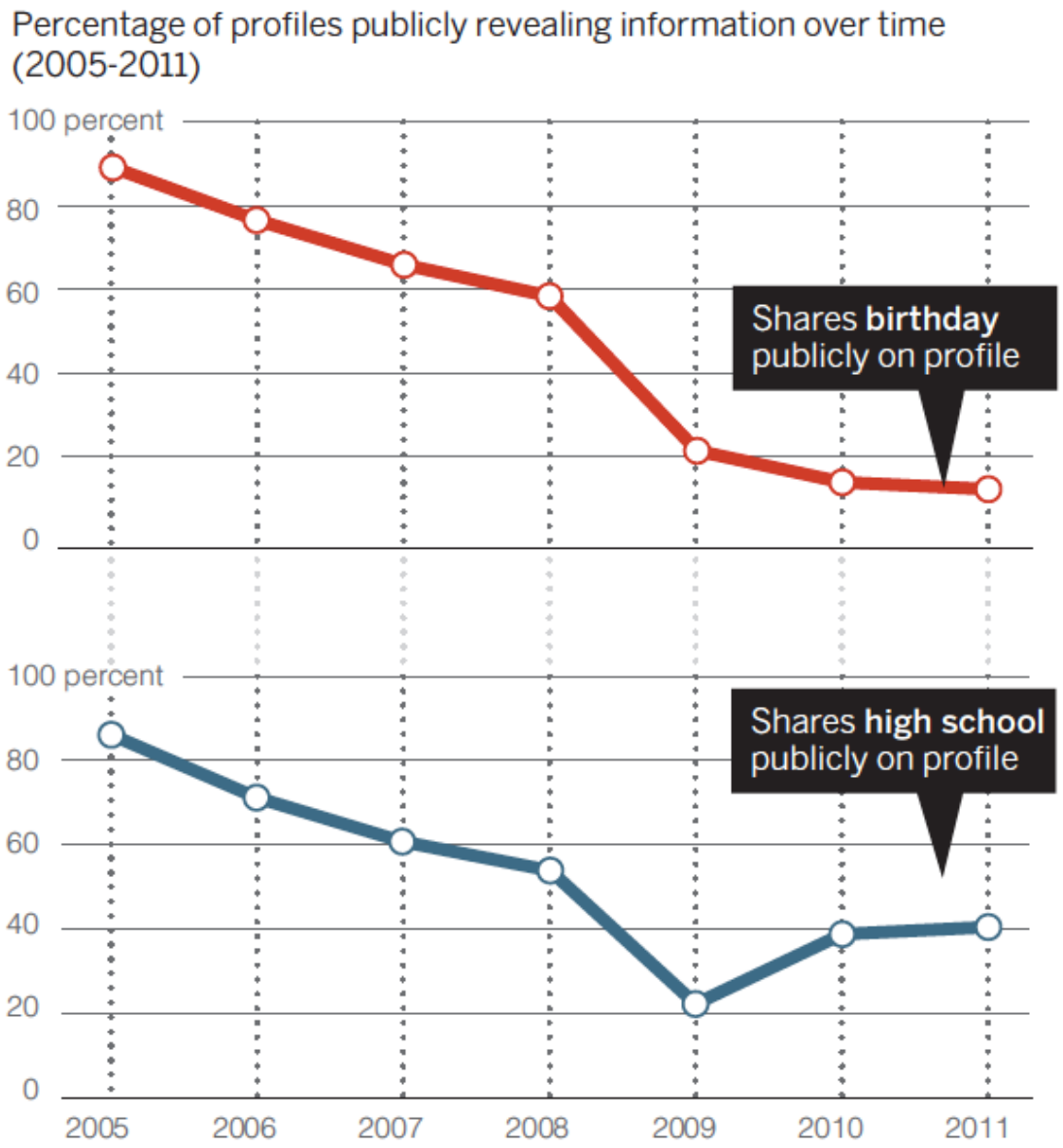
NOT VISIBLE





Disclosure behaviour in social media

Facebook:
Carnegie Mellon University students



Cambridge Analytica

- Alexander Kogan, a data scientist at Cambridge U., developed an app called "This Is Your Digital Life". He provided app to Cambridge Analytica.
- Cambridge Analytica arranged an informed consent process for research in which several hundred thousand Facebook users would agree to complete a survey only for academic use.
- However, Facebook's design allowed this app to not only collect the personal information of people who agreed to take the survey, but also the personal information of all the people in those users' Facebook social network. In this way Cambridge Analytica acquired data from millions of Facebook users.
- Steve Bannon (Vice Pres. Of CA) convinced republican megadonors to fund CA and so CA wrked for Trump’s campaign

Cambridge Analytica micro targeted ads

- Demographics: age, education, sex, …
- Psychographics: interests, opinions, values, …
- Five personality traits: openness to experience, conscientiousness, extraversion, agreeableness, and neuroticism

Send the strong terrorism ad to a 64 year old, gun-owning medium-neurotic.

He might buy a more powerful gun

How do they gather the information?

Cambridge Analytica micro targeted ads in politics

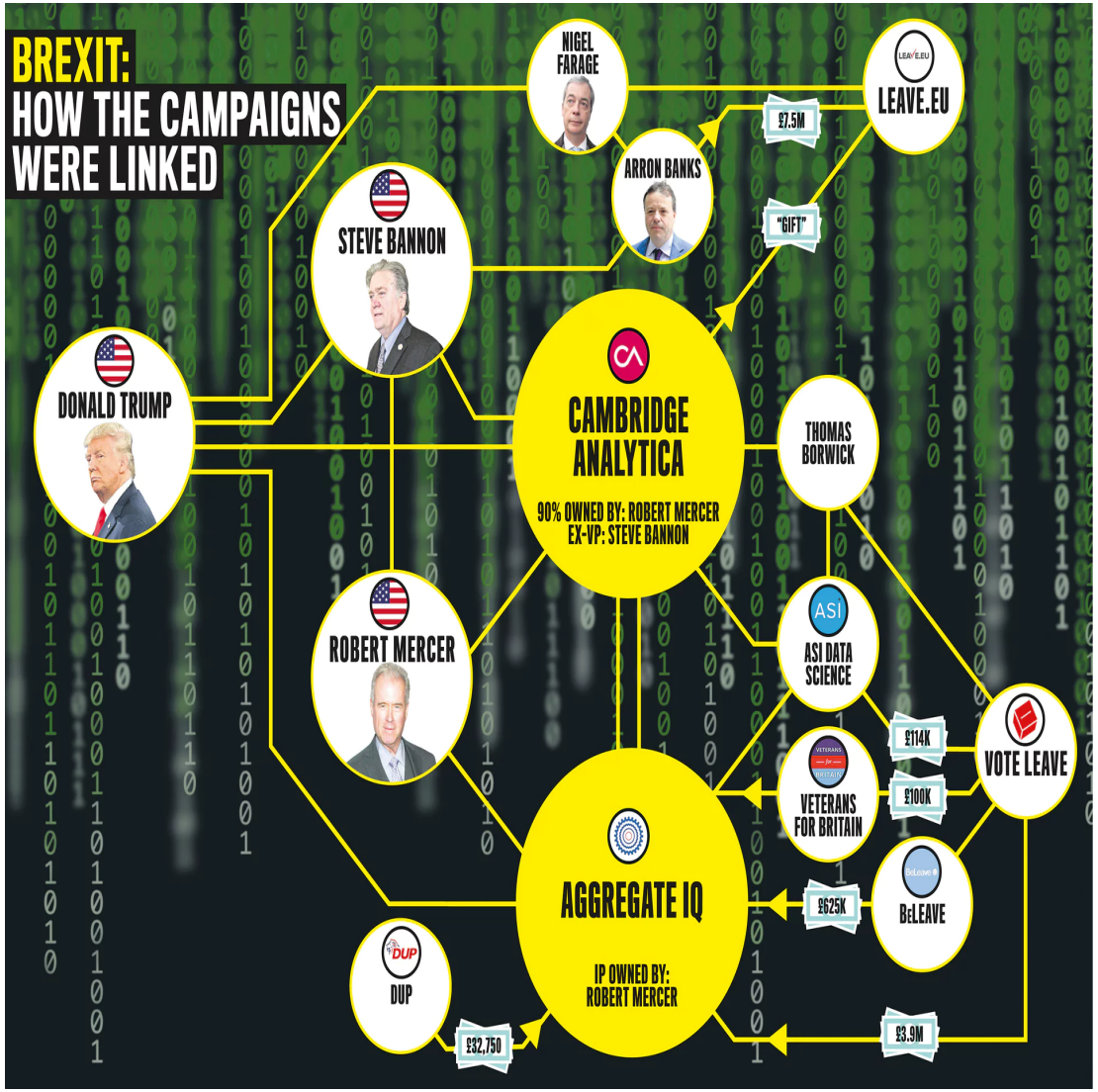
"We have profiled the personality of every adult in the United States of America—220 million people."

"We are thrilled that our revolutionary approach to data-driven communications played such an integral part in President-elect Donald Trump's extraordinary win."

Brexit, Trump campaign links

Both used the same technology

Mercer backed both with hidden contributions



Source

Cambridge Analytica: apologies

- Facebook director Mark Zuckerberg first apologized for the situation with Cambridge Analytica on CNN, calling it a "issue" , a "mistake" and a "breach of trust".
- Other Facebook officials argued against calling it a "data breach", arguing those who took the personality quiz originally consented to give away their information.
- Cambridge Analytica says the company has done nothing wrong and, so far, has appeared to cooperate with investigations.
- Cambridge Analytica said Whistleblower Christopher Wylei is misrepresenting himself and the company and strongly denies the claims made by newspapers and TV
- In 2018 Cambridge Analytica filed for insolvency proceedings and closed operations; the top people of C.A. founded Ermerdata

Cambridge Analytica how to profile

- University and the Psychometrics Center at the U. of Cambridge The studies relied on data collected by app (100-question quiz) that assessed a person's openness, conscientiousness, extroversion, agreeableness and neuroticism, traits commonly referred to in the academic community by the acronym Ocean.
- Many respondents who took the quiz authorized it to gain access to their Facebook profile data, and information about their friend network — access that was allowed by Facebook at the time.
- That allowed researchers to cross-reference the results of the quiz with the users' Facebook "likes," and build a model from the correlations they found between the two.
- With that model, the researchers could often make precise guesses about subsequent users' personalities using only a list of their likes, no 100-question quiz necessary.

Cambridge Analytica: how to transform clicks in votes

- In that study, the researchers compared the accuracy of their model with personality assessments made by the respondents' friends. The friends were given a 10-question version of the myPersonality quiz and asked to answer based on their knowledge of the respondents' personalities.
- Based on a sample of more than 32,000 participants who were assessed by both the model and one or two friends, the researchers found that the model, using just 10 likes, was more accurate than a work colleague. With 70 likes, it was more accurate than a friend or roommate; with 150, more accurate than a family member; and with 300, more accurate than a spouse.

Cambridge Analytica: back to 2016 US presidential elections

- This informationcould provide important opinion concerning basic aspects on voting, and on critical political issues (e.g. immigration, protectionism, gay rughts, public health care etc.)
- These lead to 253 psycological profiles
- These opinons were used to send targeted emails to people

- Example (Wylie- whistlebower of CA)

Cambridge Analytica could craft adverts no one else could: a neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one.

Each designed to suppress their voting intention – even if the same messages, swapped around, would have the opposite effect.

Cambridge Analytica: back to 2016 US presidential elections

These opinons were used to send targeted emails to people

Example (Wylie- whistlebower of CA)

- Cambridge Analytica could craft adverts no one else could: a neurotic, extroverted and agreeable Democrat could be targeted with a radically different message than an emotionally stable, introverted, intellectual one.

Each designed to suppress their voting intention – even if the same messages, swapped around, would have the opposite effect.

Cambridge Analytica: back to 2016 US presidential elections

- Example: “Jobs in the economy” is a meaningless message.
- Everyone’s pro-jobs in the economy. So using just the message of ‘I am in favour of jobs in the economy’, you cannot differentiate yourself from your opponent. BUT
- different people have different motivations and value sets that are interrelated with their dispositions. THEREFORE
- the same blandishment can be dressed up in different language for different personalities, creating the impression of a candidate who connects with voters on an emotional level.
- 1) to a conscientious person you talk about the opportunity to succeed and the responsibility of a job;2) to an open person, you talk about the opportunity to grow as a person;3) to a neurotic person you emphasise the security that it gives to family

Outline

- Threats and Attacks: Malware
- Use of personal information
- **Defense measures**
- Threats and attcaks: deanonymization

Personal Defense Measures (1)

- "Common sense" measures: [1]
  - Use strong, unique passwords
  - Provide minimal personal information: avoid entering birthdate, address, etc.
  - Review privacy settings, set them to "maximum privacy"
    - "Friends of friends" includes far more people than "friends only"
  - Exercise discretion about posted material:
    - Pictures, videos, etc.
    - Opinions on controversial issues
    - Anything involving coworkers, bosses, classmates, professors
    - Anything related to employer (unless authorized to do so)
  - Be wary of 3rd party apps, ads, etc. (P.T. Barnum's quote)
  - Supervise children's OSN activity

Personal Defense Measures (2)

- More advice [1]:
  - "If it sounds too good to be true, it probably is"
  - Use browser security tools for protection:
    - Anti-phishing filters (IE, Firefox)
    - Web of Trust (crowdsourced website trust)
    - AdBlock/NoScript/Do Not Track Plus
  - Personal reputation management:
    - Search for yourself online, look at the results…
    - Google Alerts: emails sent daily to you about results for any search query (free), e.g., your name
  - Extreme cases:
    - Cease using OSNs, delete accounts
    - Contact law enforcement re. relentless online harassment

Discussion questions

- *Who should* protect your privacy?
- Costs of privacy
- Interaction with technologists
- Privacy attitudes and privacy behavior

Who should protect your privacy?

- Self-regulation?
- Individual responsibility?
- Policy/legislation?
  - EU vs. US (next lecture)

The costs of privacy

- Costs incurred by business and individuals due to incomplete or insufficient privacy protection
  - Individuals: do not protect themselves
    - (*Should* they?)
  - Other parties: do not internalize costs
- Costs: tens of billions dollars every year (also many new jobs….)
- Example -2015: AT&T wants its customers to pay $29 a month not to have their online activities monitored analyzed and used for advertisements when signing for Giga power service

Privacy attitudes and privacy behavior

- Attitudes: Usage
  - Top reason for not going online (Harris)
  - 78% would increase Internet usage given more privacy (Harris)
- Attitudes: Shopping
  - $18 billion in lost e-tail sales (Jupiter)
  - Reason for 61% of Internet users to avoid ECommerce (P&AB)
  - 73% would shop more online with guarantee for privacy (Harris)
- (most of the above is 2001 data…)
- Attitudes: Experiments
  - Chellappa and Sin 2002: *c*onsumer's intent to use personalization services positively influenced by trust in vendor
  - Il-Harn, Hui, Lee, and Png 2002: protection against errors, improper access, secondary use worth $30.49 – 44.62 to American users

Privacy attitudes and privacy behavior

- Rationality assumption you give up privacy for economic return (e.g. free app if you give your data)
  - Economics of privacy: rational agents:
- Immediate gratification: we overstimate the advantage of immediate gratification neglecting future loss
- Anecdotic evidence

  "Ask 100 people if they care about privacy and 85 will say yes. Ask those same 100 people if they'll give you a DNA sample just to get a free Big Mac, and 85 will say yes." Austin Hill

Privacy attitudes and privacy behavior
A rational agent

$$\max_{d} U_t = \delta \left[v_E(a), p^d(a) \right] + \gamma \left[v_E(t), p^d(t) \right] - c_t^d$$

- U = utility at t, d decision taken
- $v_E(a)$ = payoff (gain) to keep a private (< 0 if a is revealed)
- $v_E(t)$ = payoff (gain) to use technology t (< 0 if a is revealed)
- c_t = cost time t for decision d
- $P_{d(a)}$ probability a is revealed if decision d is taken

Privacy attitudes and privacy behavior
A rational agent

$$\max_{d} U_t = \delta \left[v_E(a), p^d(a) \right] + \gamma \left[v_E(t), p^d(t) \right] - c_t^d$$

Problems

- Incomplete information
- Bounded rationality
- Hyperbolic discounting

Privacy attitudes and privacy behavior
A rational agent

$$\max_{d} U_t = \delta \left[v_E(a), p^d(a) \right] + \gamma \left[v_E(t), p^d(t) \right] - c_t^d$$

Incomplete information

- Do we know values of possible profit?
- Do we know costs of privacy costs?
- These costs are perceived
- Companies try to hide real values

Privacy attitudes and privacy behavior
A rational agent

$$\max_{d} U_t = \delta \left[v_E(a), p^d(a) \right] + \gamma \left[v_E(t), p^d(t) \right] - c_t^d$$

Bounded rationality

- Psycological aspects
- Too many variables
- Incomplete information availbale to users

Privacy attitudes and privacy behavior
A rational agent

$$\max_{d} U_t = \delta \left[v_E(a), p^d(a) \right] + \gamma \left[v_E(t), p^d(t) \right] - c_t^d$$

Hyperbolic discount

- Human beings understimate the future and favour better playoff in the present

Example: two possibilites

1. work extra 4 hours tomorrow
2. Work extra 5 hours next week

Most people choose 2

Privacy attitudes and privacy behavior Conclusions

- Rationality model are not appropriate to describe individual privacy behavior
- Time inconsistencies lead to under protection and over release of personal information
- Genuinely privacy concerned individuals may end up not protecting their privacy
- Also sophisticated users will not protect themselves against risks
- Large risks accumulate through small steps
- Not knowing the risk is *not* the issue