Two tales of privacy in OSNs

Claudia Diaz
KU Leuven ESAT/COSIC

Guest lecture
TU Darmstadt, February 12, 2013

based on joint paper with Seda Gürses, accepted at IEEE S&P Magazine
Outline

• Two narratives: the activist and the consumer

• Two ways of framing privacy
  – Understanding and improving social privacy in OSNs
  – PETs for social networks: evading surveillance and censorship

• Comparison of approaches
  – Surveillance and social privacy problems treated as unrelated
    • abstract away the complexity of the privacy problem
  – Challenges for integration of approaches?
  – Points for discussion
Facebook and Twitter key to Arab Spring uprisings: report
Carol Huang
Jun 6, 2011

DUBAI // The most popular Twitter hashtags in the Arab region in the first three months of this year were "Egypt", "Jan25", "Libya", "Bahrain" and "protest".

Nearly 9 in 10 Egyptians and Tunisians surveyed in March said they were using Facebook to organise protests or spread awareness about them.

All but one of the protests called for on Facebook ended up coming to life on the streets.

These and other findings from the newly released second edition of the Arab Social Media Report by the Dubai School of Government give empirical heft to the conventional wisdom that Facebook and Twitter abetted if not enabled the historic region-wide uprisings of early 2011.

In part by using the social networking sites, activists organised and publicised the unprecedented protests that gave rise to the so-called Arab Spring, which has so far seen longtime governments in Egypt and Tunisia fall, regimes in Syria, Libya, Yemen and Bahrain clash with the opposition, and leaders in Jordan, Saudi Arabia and the UAE offer more benefits to their populace.

Twitter Revolution: How the Arab Spring Was Helped By Social Media
Saleem Kassim in World, Middle East 5 months ago

As a result of the many technological advancements and innovations that have revolutionized how individuals communicate, an abundance of information has become available to everyone. Depending on where the information is found, however, it's reliability can be questioned. With the growing number of international, self-described (both non-for-profit and for-profit) organizations such as Facebook, Wikipedia, Wikileaks and more, much of the information provided is now often opinionated and biased, nonetheless, truthful.

Ultimately, public information supplied by social networking websites has played an important role during modern-day activism, specifically as it pertains to the Arab Spring. In Arab countries, many activists who played crucial roles in the Arab Spring used social networking as a key tool in expressing their thoughts concerning unjust acts committed by the government.

Being capable of sharing an immense amount of uncensored and accurate information throughout social networking sites has contributed to the cause of many Arab Spring activists. Through social networking sites, Arab Spring activists have not only gained the power to overthrow powerful dictatorship, but also helped Arab civilians become aware of the underground communities that exist and are made up of their brothers, and others willing to listen to their stories.

In countries like Egypt, Tunisia, and Yemen, rising action plans such as protests made up of thousands, have been organized through social media such as Facebook and Twitter. “We use Facebook to schedule the protests” an Arab Spring activist from Egypt announced “and [we use] Twitter to coordinate, and YouTube to tell the world.” The role that technology has taken in allowing the distribution of public information such as the kinds stated by the aforementioned
The positive narrative

• Social media enabler for social change, for citizens to contest ruling institutions, to foster democracy and human rights, ...
  – Conveniently, the companies providing these social media services originate from the USA

• One line of criticism to this narrative: role of SM is exaggerated, more credit to organization and events on the ground
If the Riots Resume, Will the UK Try to Block Social Media?

By Jeremy Kirk, IDG News Service
Aug 12, 2011 6:10 AM

Scrambling to deter future violent rioting, the U.K. government is considering shutting down social networks such as Twitter and Facebook during civil disturbances, but the heavy-handed proposal is already drawing criticism.

Social networks and services such as the BlackBerry Messenger application were employed by some rioters to communicate, which lead Prime Minister David Cameron on Thursday to propose "whether it would be right to stop people communicating via these websites and services when we know they are plotting violence."

The approach is similar to measures taken by governments such as Egypt and Tunisia, both of which sought to restrict Internet access and services to quell anti-government demonstrations.

"Nobody can believe the government is serious," said Jim Killock, executive director of the Open Rights Group, a nonprofit technology watchdog organization. "Clearly Twitter and BlackBerry and other tools have been used for good purposes as well as ill."

The Kremlin makes its move on Facebook

13 Jul 2012

Russian parliamentarians have passed legislation that will establish a central register of banned websites. The new laws are ostensibly designed for child protection, but Andrei Soldatov says the real aim is to take control over the country's burgeoning social networks.

READ: INDEX CONDEMNS RUSSIAN INTERNET BLACKLIST PLAN

On 11 June the Russian State Duma passed amendments to the laws 'On the protection of children from information deemed harmful to their health and development', 'On information', 'On communications' and the Code of Administrative Offences at the second and third readings. The main gist of the draft law is that from 1 November this year Russia will have a single register of sites and web pages to be blocked ("Single Register of domain names, internet page selectors and URLs identifying sites in the internet containing information banned in the Russian Federation").

For the first time the Kremlin will have at its disposal the facilities for blocking access to internet resources across the whole of Russia.

The principle of internet censorship is, of course, not a new one to the Russian authorities. For some five years now, regional and city prosecutors have been busy implementing regional court decisions that required providers to block access to forbidden sites. Up until now this has been done unsystematically, so that sites blocked in one region remained accessible in others. The Register, which is to be compiled by a special federal organisation, will remove this problem.

Syria's Internet Connection Gets Cut Off

Published: Thursday, 29 Nov 2012 | 2:35 PM ET
By: Cadie Thompson
Technology Editor, CNBC.com
Governments are increasing cyber security on social media

by paganinip on August 1st, 2012

Many experts are sure, the new horizons of intelligence are in the social media and in the ability to control them. Governments are more careful on the analysis of social media and the vast amount of information which they hold.

Intelligence agencies have learned that Social networks and forums are exceptional instruments for information gathering and to measure the global sentiment on every kind of argument, political as social.

Last Week the Intelligence community veterans said at a panel discussion on open-source intelligence hosted by Government Executive.

| "We take a large look at the world and see if there's a surprise out there," |
| said Patrick O’Neil, analytic director of the Open Source Center for the Office of the Director of National Intelligence. |

| "We’re trying to avoid a surprise." |

O’Neil with his words highlights the great importance that intelligence community assigns to the social media and to the open source intelligence, they offer a vantage point of today’s society.

The new way to make intelligence is considered in opposition with the previous methodologies, today intelligence is primary based on open source intelligence contrary to the past when the intelligence was based on clandestine sources.

Increasing Concerns on Social Media Monitoring, from Governments to Private Businesses

Pierluigi Paganini November 06, 2012

Whenever we surf on the web we disseminate a large amount of information that could be used for different purposes. Contrary to what you might believe, this information is very precious for private businesses and government agencies. The first group uses them mainly for commercial analysis; the second for monitoring and surveillance.

The user has the wrong perception that vast majority of web services are offered free of charge. Facebook, Twitter, and YouTube increase the number of their users every day, and collect an incredible amount of data to be used for analysis of various types.

New horizons of intelligence are in the social media and in the ability to control them. Governments are more careful on the analysis of communication platforms and the vast amount of information which they hold. Intelligence agencies have understood that social media represent a privileged instruments for information gathering and mass-conditioning.

The social media are vital component in today’s intelligence analysis, but if it is quite simple for governments to acquire a huge quantity of data, their elaboration is not so simple. We must consider that due to the possibility of pollution of the sources by the same intelligence agencies, the information might not have the proper level of reliability.
LONDON — Syria is using equipment and software developed by an American company to censor the Internet and conduct surveillance of its citizens, according to data analyzed by technology experts and advocates for Syrian dissidents.

The equipment, developed by California-based Blue Coat Systems, is allegedly being used by Syria’s autocratic government to block access to the Internet and crack down on dissidents who have been protesting against President Bashar al-Assad for nearly eight months, the experts and advocates say.

We explain that Facebook, Twitter, YouTube, and a host of other social networking platforms are increasingly viewed by intelligence agencies as invaluable channels of information acquisition. We base our findings on three recent case studies, which we believe highlight the intelligence function of social networking. (Joseph Fitsanakis, Research: Spies increasingly using Facebook, Twitter to gather data, intelNews.org, February 13, 2012)[below is article]

By JOSEPH FITSANAKIS | intelNews.org |
During the past four years, this blog has reported several incidents pointing to the increasing frequency with which spy agencies of various countries are utilizing social networking media as sources of tactical intelligence. But are we at a point where we can speak of a trend? In other words, is the rapid rise of social networking creating the conditions for the emergence of a new domain in tactical intelligence collection?
Facebook Censors Breastfeeding Moms

After Facebook's L'Homme du Jour censorship fiasco in January, you would think the social networking giant would have deciphered the difference between "indecency" and innocent, non-pornographic images.

Apparently not. Facebook has been taking flack over widespread censorship of photos of breastfeeding mothers.

Censorship has been widespread. In Belleville, Ontario, the Facebook page of a support group breastfeeding mothers hosted by the local Ontario Early Years Centre has had its pictures deleted by Facebook's administration. As one member of the group had to say,

"It's the most natural thing to do for your baby, and Facebook says its indecent? We're just a small group, but Facebook is still censoring some of our images. Even though its a page specifically about breastfeeding."

Individual accounts have also been suspended for uploading photos of their children breastfeeding. Emma Kwasnica, a breastfeeding mother of three, had her account suspended over the weekend. As she told the Huffington Press on Sunday, she can stand Facebook's hypocritical stance over her choice to breastfeed,

"It's such a double-standard: if you type in 'breasts' on Facebook, you can see pages with thousands of members where there are naked breasts. How is that happening, when at least 30 women I know have had accounts shut down for a single.

Is Facebook Censoring Your Comments?

May 07, 2012 4:42 PM EST

By Fahmida Y. Rashid

A strange thing happened to Robert Scoble, a fan of all-things-social, over the weekend when he tried to comment on a Facebook post. Facebook blocked his comment outright, calling it "irrelevant or inappropriate."

It's no secret that Facebook monitors comments to block spam and offensive content. Users can flag inappropriate images or comments for Facebook to remove. If a user is reported too many times, they are no longer allowed to post on the site. It also blocks friend requests from being sent if it looks like spam because the two users don't have many friends in common. There've also been reports of people being temporarily blocked from posting on the site entirely after writing too many comments within a short period of time.

However, the error message sounded as if Facebook was analyzing the contents of the message and deciding what was relevant or not, which would go beyond traditional anti-spam measures and veer into censorship territory.

"Wow, does Facebook do sentiment analysis on comments and keeps you from posting negative comments?" Scoble asked on his Facebook page.
Facebook's Privacy Issues Are Even Deeper Than We Knew

Questions about what social networks mean for personal privacy and security have been brought to a head by research at Carnegie Mellon University that shows that Facebook has essentially become a worldwide photo identification database. Paired with related research, we’re looking at the prospect where good, bad and ugly actors will be able identify a face in a crowd and know sensitive personal information about that person.

These developments mean that we no longer have to worry just about what Facebook, Google+, LinkedIn and other social sites do with our data; we have to worry about what they enable others to do, too. And it now seems that others will be able to do a lot.
The negative narrative

• How governments exploit SM:
  – Social media blocked during civil unrest to prevent communication
  – Social media used to disseminate misinformation or propaganda
  – Social media used to spy on people
    • Information can be used to, eg, identify (and arrest or kill) dissenters

• Collusion SM companies and governments (particularly USA government)
  – The “surveillant assemblage”

• Link to technologies:
  – how to design technologies with which people can interact socially online while being free from surveillance and interference (eg, censorship)
Other perspectives on the problem of privacy in OSNs

• Safety, protection from crime
  – The bad guys: malware, scammers, online thieves, predators, stalkers
  – The good guys: regulators, industry, and law enforcement
  – Technologies: data security, software security, authentication/identification, access control, monitoring
  – Privacy issues ~ data security issues

• Data protection
  – Purposes for which information is used
  – Informed consent
  – Data portability
  – Subject access rights (eg, deletion)

• Social privacy
  – OSNs are spaces to socialize – unsurprisingly, all the privacy issues of social relationships reappear, plus new ones that appear
The Wrong Facebook Comments can Get You Fired!

Writing the wrong comments on Facebook has resulted in some people losing their jobs!

There are numerous examples of people losing their jobs and messing up their careers because of comments they made on Facebook.

Facebook is a wonderful social networking site but you have to be very careful.

These people I have written about below thought they were having a private moan about their boss or job to their friends on Facebook.

They were mistaken and it got them fired!

You will be amazed at some of the stupid comments that people post on Facebook!

When you read about some users of Facebook whose comments got them sacked from their jobs you will be surprised at just how idiotic and naive they were!

Moaning about your job

Before the creation of the internet and social networking sites like Facebook we would all have a moan about our jobs, bosses and careers. We’d come home and tell our mates or family about the terrible day we had at work.

We’d go on about the stupid irritating or boring things our boss wanted us to do during our working day.

How To Lose a Job Via Facebook In 140 Characters or Less

Posted by Mark in Career, News, Social Media on 08 9th, 2009 | 285 responses

These days social media and job search go hand in hand. Of course the age old knock on the door and “are you hiring?” scenario is still out there but many people favor job search via networking and making use of online job search sites.

Over the years networking platforms such as Twitter, Facebook and LinkedIn have become a must for job seekers. If you aren’t on the web, at times it’s almost impossible to secure a job. However, some people seem to keep forgetting that social media if not utilized properly can hurt your job search and can lead to job loss. We came across one and had to share it.

Please take a look at the image below,

The image above clearly shows the implications if you use social media platforms the wrong way. Of course, when you have a Facebook account it’s your personal account. However, it depends how you are using it. Are you using it to simply connect with your friends and family or are you using it to connect with professionals? Before you go ahead and utilize the power of free speech on Facebook or any other social media platforms make sure you watch what you are saying. Social media has given us tremendous amount of power in terms of job search but it has also made everything we do much more vulnerable. The saying “choose your words carefully” might
Employers Asking for Facebook Passwords

By Alison Doyle, About.com Guide  August 11, 2012

In another twist on employers checking out candidates on social networking sites there are reports of employers asking for the Facebook passwords of job applicants and, in some cases, for current employees. Checking social media sites this way is called "shoulder surfing" because the employer is seeing everything you do, rather than just the public information you want them to see.

If this happens to you, all the work you may have done on adjusting your privacy settings to limit what some of your friends, family and others can see is basically useless. Once you have given out your login information, the company will have full access to your account.

Should employers be asking job applicants for Facebook passwords? In my opinion, they shouldn’t. There should be a line between personal and private and this would seem to violate it. In addition, giving out passwords to any of your online accounts isn't a good idea, because whomever you give it to doesn't just have the ability to view your account. It gives them full access.
Facebook outs gay University of Texas students to their fundamentalist fathers

Posted on October 15, 2012 by John Wright

Taylor McCormick, a native of Blanco, Texas, is one of two gay UT students who were outed to their parents when they were added to the Queer Chorus' discussion group. (Photo by Lance Rosenfield)

In case you missed it, and in what almost seemed like a sick nod to National Coming Out Day, The Wall Street Journal on Saturday published a harrowing tale about two University of Texas at Austin students who were outed as gay to their fundamentalist fathers as a result of a privacy loophole on Facebook.

Basically, both students had joined UT's Queer Chorus, whose president added them to its Facebook discussion group, not knowing that it would bypass their individual privacy settings and share the information with their parents.

The disclosure prompted one of the student's fathers to call her repeatedly, threatening to stop paying her car insurance and demanding that she go on Facebook and renounce both the chorus and homosexuality.

"To all you queers. Go back to your holes and wait for GOD," the girl's father wrote on his own Facebook page. "Hell awaits you pervert. Good luck singing there."

The father of the other student, who's from Blanco, Texas, didn't talk to him for weeks.

Facebook privacy loophole allows profile stalking

Summary: A new Facebook privacy loophole has been discovered that allows you to stalk someone's profile. The flaw is related to how Facebook treats deactivated accounts and needs to be fixed asap.

Survey: Large Number Of Parents Spy On Their Children On Facebook

Caitlin Fitzsimmons on October 19, 2010 12:49 PM

Concerned about privacy on Facebook? If you're a teenager, you might want to look at your parents.

A new survey by privacy firm TRUSTe suggests that parents of Facebook-using teens actively monitor what their children post on the social networking site. One in 10 even secretly log into their kids’ accounts without permission.

The survey of 1,000 parents whose teenage children are actively using Facebook found people were generally pretty comfortable with the site's privacy policies and settings. However, it seemed that this complacency might be based on false assumptions.

Are Parents Addicted To Spying On Their Kids?

Kids are desperate to flee from their parents' spying, reports the Wall Street Journal. In a piece about “Tweens' Secret Lives Online,” the Journal tracks the online lengths kids are going to in order to get away from their stalkerish parents.

Digital anthropologist danah boyd told me last year that teens then were fleeing from Facebook to Twitter to escape the prying eyes of adults, WSJ journo Katherine Rosman says that Instagram is now one of the tools kids use to exchange messages in a semi-public way (where the public doesn’t include nosy adults).
Social privacy issues

• context collision (family, friends, colleagues)
• unintended (or “unexpected”) information disclosures
• information taken out of context
• misconfiguration of privacy settings (not usable)
• open settings overriding more restrictive settings
• software bugs
• unintended mistakes (upload wrong picture of video)
• bad decisions: regrets (angry, not thinking)
• “inappropriate” comments or content

• Other issues
  – coercion (to provide password)
  – notice and choice (informed consent) model: difficulty to read / understand privacy policies
Social privacy research

• Understand social privacy issues from a user / community perspective, and its interrelation with technology design

• Improve OSN design based on user values
  – system is intuitive, easy to use
  – behaves according to user expectations
  – helps users make better privacy decisions
  – provides meaningful privacy controls
  – has appropriate privacy defaults
  – nudges the user towards better behavior
  – supports users and communities in developing privacy practices
Privacy practices

• “privacy is a social construct that reflects the values and norms of everyday people” (boyd)
• tensions between privacy and publicity
• negotiating boundaries between the private and the public
• negotiating acceptable and unacceptable forms of behavior

• OSN architecture influences practices (boyd):
  – Persistence: Digital expressions are automatically recorded and archived
  – Replicability: Digital content is easily duplicated
  – Scalability: The potential visibility of digital content is great
  – Searchability: Digital content is often accessible through search engines
Practices and strategies

• etiquette: bad taste to comment on pictures that were uploaded years before
• indicating who is the audience (through the use of language, based on topic)
• use of settings (blocking content towards certain people who may criticize or make fun of it)
• separate profiles (in one or several OSNs)
• account deactivation while offline
• regular deletion of content
• Social steganography: “encoded” messages that mean different things to different people, obscure references, inside jokes

• How does OSNs design impact these practices and strategies?
Increasing transparency and improving privacy relevant decision-making

• Privacy is about “people being able to make informed decisions wrt information disclosure”

• System behaves according to their expectations

• Users have meaningful controls

• Users are nudged to be protective of their privacy (make it easy to be more private)
First decision: to join the OSN

- Do users read the privacy policies?
  - Mostly not, even less understand them
  - Warning: privacy policies used as disclaimer to then do whatever they want with the data! once the user accepts the policy, she consents to its terms

- How to improve the readability of privacy policies?
  - easy to find and interpret, to the point, standardized?

Survey: Facebook, Google privacy policies are incomprehensible

Summary: Facebook and Google privacy policies have been found to be more confusing than complex documents such as government notices, credit card agreements, and bank reward-program rules.
Make privacy information salient

- Privacy policies of websites, apps, etc.

Slide: Lorrie Cranor
Make it easy to segregate audiences

• Access control policies designed for sys admins
  – Now everyone must be able to configure privacy settings (a type of AC policy)

• Goal: reduce cognitive load of user

• Better interface designs for grouping friends
  – closer to the users mental models

• Automated grouping of friends
  – leverage user attributes, social graph properties (eg, clustering), past interactions
Make audience visible

• Current privacy settings, access control settings

• Consequences of sharing
Make it easy to select privacy

- Settings that default to privacy
- Usable privacy controls and tools
- Add friction to privacy-reducing options
  - More clicks, scrolling, delay

Are you sure you want to make your photo public?

No  Yes
Regret studies

• Series of studies: interviews, diary study, surveys
  – Focus on American users of Facebook and Twitter
  – Data collected from over 3000 social network users
    • Interviews with Pittsburgh residents
    • Large survey samples from Amazon Mechanical Turk

• Research questions
  – How common is it to have social network regrets?
  – What do users regret doing on social networks?
  – Why do users take regrettable actions?
  – What are the consequences of these regrettable actions?
  – How do users avoid or repair regrets?
  – How are regrets different on social networks and in conversations?
Overview of findings

• Most social network users reported regrets
  – 57% of FB users reported FB regrets
  – 51% of Twitter users reported Twitter regrets
  – 79% of Twitter users reported conversational regrets

• Serious consequences
  – Relationship breakup, job loss
  – Less serious consequences still very upsetting

• Underlying causes often included being angry or upset, not thinking, or forgetting who might read their posts

• Most regrets occurred within one day of posting


Other papers under review
What do people regret on FB?

• Posts about
  – Personal information/issues about themselves or others
  – Sex
  – Relationships
  – Profanity
  – Alcohol and drug use
  – Jokes
  – Lies
  – Information about work or company

• Friending and unfriending
• Photo tagging
• Using Facebook applications
Why did they do it?

• Excited state
  – Negative: Angry, bad mood, venting
  – Positive: Happy, share good news
• Didn’t think
• Unintended audience
• Thought it was cool or funny
• Under the influence of alcohol or drugs
• Didn’t mean to post it
Timer nudge (stop and think)

You will have 10 seconds to cancel after you post the update

Your post will be published in 3 seconds. Post Now | Edit It | Cancel

slide: Lorrie Cranor
Sentiment nudge (content feedback)
Profile picture nudge (audience feedback)

This is a public post.

These people and ANYONE ON THE INTERNET can see your post.
Preliminary results

• Timer nudge
  – Overall perceived as useful
  – Users reported rephrasing/correcting/canceling posts

• Profile picture nudge
  – Overall perceived as useful
  – Made users more aware of audience and number of FB friends
  – Reminded users to use the appropriate privacy settings

• Sentiment nudge
  – Positive sentiment nudge was deemed useless
  – Negative sentiment nudge annoyed people: missing context, misinterpreting sarcastic comments, judgmental, censoring
  – Need smarter sentiment analysis algorithm and better messaging

slide: Lorrie Cranor
Social privacy: methodology

• Research often based on user studies
  – Qualitative (small scale) studies based on user interviews
  – Quantitative (larger scale) studies, extract statistics

• The studies help:
  – understand user expectations and concerns
  – study the impact of different design options

• Big issue: how representative is the user sample?
  – of collectives with specific needs/situations
  – in other countries
Back to surveillance and censorship concerns...

Research in cryptography and computer security: Privacy Enhancing Technologies (PETs) for OSNs
PETs methodology

• Model the system, make explicit assumptions (eg, trust assumptions, available building blocks)

• Identify the threat model (knowledge, access, capabilities)

• Identify the information to protect (eg, content, traffic data) and the type of security property (eg, confidentiality, availability)

• Perform a security analysis of the system to test if the security properties hold, and under which circumstances (assumptions)
Accessing censored sites

- Use of Tor (or other anonymous communication networks) to access blocked OSN sites
  - even better if the circumvention is undetectable

Tor Project Wins Award for Role in Middle East Revolutions

The Tor Project has been recognized by the Free Software Foundation for its role in the protests and revolutions around North Africa and the Middle East.

This software, which allows for safe and anonymous web browsing, was given the FSF’s Award for Projects of Social Benefit. The award is intended to highlight “a project that intentionally and significantly benefits society through collaboration to accomplish an important social task.”

Without question, enabling the Internet’s role in political revolution has been an important social task, and one that the Tor Project has explicitly supported. In its section on activist users, Tor reps state that anonymous browsing is essential for reporting abuses of power and organizing protests, especially from behind government-sponsored firewalls and ISP blocks.

Activists in Tunisia, Egypt and Bahrain told CNN about five technologies that have been most useful in getting around government-imposed blockades:

1. Tor

Tor is a circumvention tool that allows users to access censored information online, by bouncing communications among a network of users around the world, ultimately enabling its users to maintain anonymity online.

Slim Amamou, a “hacktivist” based in Tunisia, describes Tor as a program that enables you to “circumvent the central service of censorship by using a computer from someone else in the world.”

It played a crucial role, he says, because social media pages sharing information about the protests were “systematically censored so you could not access them without censorship circumvention tools.”

“So [Tor] was vital to get information and share it.”

U.S. Secretary of State Hillary Clinton said restrictions on Internet activity that prohibit free expression are among the most worrisome trends concerning human rights.

Yet as governments become more savvy in their attempts to repress freedom of expression on the Internet, their citizens have become cyber-sleuths, creating innovative technologies to circumvent censors and authorities tracking their Internet activities.
Protecting content

• Use encryption: diversity of tools
  – Note: main difference with settings is the protection from OSN provider
  – FlyByNight:
    • Facebook app that protects user data by storing it encrypted
    • Relies on FB for key management
  – Scramble
    • Browser plug-in that encrypts content prior to uploading
    • Key management done out of band

• Issues:
  – usability, flexibility of interface
  – key distribution (network effect – critical mass needed)

• Bonus
  – encrypting the content makes censorship of content more difficult
Initialization:

Key pair: \[
\begin{cases}
\text{Public key pair (Encryption and signing): } pk \\
\text{Secret key pair (Encryption and signing): } sk
\end{cases}
\]

Posting content: A message \( m \)

\[
F = \{\text{Alice, Bob, Carol, Diana}\}
\]

\[
\sigma_m \leftarrow \text{Sign}(m, sk_A)
\]

\[
k
\]

\[
C \leftarrow \text{Enc}_k(\sigma_m||m)
\]

\[
m' \leftarrow \{\text{Enc}_{pk_{Alice}}(k)||\text{Enc}_{pk_{Bob}}(k)||\text{Enc}_{pk_{Carol}}(k)||\text{Enc}_{pk_{Diana}}(k)||C^8\}
\]
OSN may not like encrypted content

• Q: should the law establish a right to encrypt the content users store/share in a service?
  – Or should the OSN provider have the right to say “If you use my service, I must be able to look into your content”?
    • Compare to offline services (post, phone calls, cafes)
  – Issues:
    • “inappropriate” content (censorship?)
    • conflict with business model
Steganography?

- Not possible for the OSN provider to realize that the content is encrypted

- NOYB (None Of Your Business)
  - substitute (shuffle) user attribute values (age, location, etc.)
  - only users with the right keys can ‘undo’ the shuffle and retrieve the real attribute values

- FaceCloak
  - symmetric key (shared only with audience of content) to encrypt user’s information in Facebook
  - encrypted data is stored in the FaceCloak server, and replaced in Facebook by random text fetched from wikipedia.
  - The random text acts as an index to the encrypted data on the server.

- Issues
  - misrepresentation of user interests towards the OSN provider (who still performs profiling on the noisy information) and towards other users who might not be using the system
  - undetectability of the tool: double-edged sword
Protecting relationships and interactions

• Even if content is encrypted, valuable intelligence can be extracted from analyzing the social graph and the fine-grained interactions of users

• Is anonymity an option for online social networking?

• Obfuscation of relationships/interactions with dummy traffic
  – content encrypted: hard to distinguish encrypted content from random data (dummies)
    • Difference with obfuscating plaintext?
  – Dummy traffic expensive: how to optimize dummy traffic generation?
    • Metrics to assess the effectiveness of dummy traffic (eg, mutual information)
Alternative centralized architectures

• HummingBird
  – privacy-enhanced alternative to Twitter
  – relies on a set of crypto protocols
  – “protects tweet contents, hashtags and follower interests from the (potentially) prying eyes of the centralized server”

• Use the OSN as a “dumb” data store for encrypted blobs
  – Client software stores and retrieves blocks, and organizes info for presentation to the user

• No protection against traffic analysis
Distributed architectures

• Adversary model in centralized OSNs is very strong:
  • global, potentially active
  • protection against traffic analysis very hard

– Distributed architectures?
  • Diaspora, Safebook, Peerson
  • Challenges:
    – information availability, synchronization, security of client software
    – adversary and traffic analysis guarantees difficult to model
Challenges for integration: who?

- **Who defines what the privacy problem is?**
  - experts: based on their technical knowledge (techno-centric)
    - Plus: what is technically possible? How can information be abused?
    - Limitation: how do these technical risks map to social/political analyses of surveillance practices?
    - Limitation: technical tools do not behave as predicted in different contexts (social practices)
    - Limitation: no emphasis on usability, user needs

  - users: based on their perceptions and experiences (user-centric)
    - Plus: take into account user perspective, context
    - Limitation: biased samples (often people in the US or EU), would a dissenter in Egypt have the same concerns as college student in the US?
    - Limitation: no insight into organizational practices
    - Limitation: users have a limited understanding of the technical infrastructure

- regulation: based on legal norms (organization-centric)
  - Limitation: compliance with data protection regulation does not necessarily imply privacy protection
Challenges for integration: what data?

• What information is in the scope of the ‘privacy problem’?
  – social privacy: emphasis on user-generated content, volitional actions (no implicit data)
    • how to communicate to users issues derived from implicit data?
  – PETs: in principle, all data is in the scope (volitional and implicit)
    • BUT: risks only with respect to the adversary (not ‘friends’)
    • Content-agnostic: does not take into account the semantics of the content (semantics and context are however very relevant for social privacy)
Challenges for integration: how are privacy problems identified/defined?

- **Social privacy**
  - focus on concrete harms in the user (social) environment
  - intuitive causality between disclosures and consequences

- **PETs**
  - focus on risks that might lead to ‘abstract harms’ (worst-case scenarios)
    - individual harms: being arrested, put under surveillance, inferences of sensitive information, intrusion, manipulation
    - societal harms: discrimination, surveillance society, information asymmetry, upsetting existing checks and balances of power between individuals, state and private sector

- **Issues**
  - No information (transparency) about what is actually being done with the data
  - How to communicate abstract harms to users?
Example difference: concept of time and disclosure

• Confidentiality: “preventing unauthorized access to information from unauthorized entities (persons or machines)”

• In PETs:
  – monotonic property (no “taking back”):
    • once disclosed, forever disclosed
    • even if in practice it was never ‘accessed’ by the unauthorized party

• In social privacy (access control settings)
  – over time, information can be disclosed and then become confidential again (change of settings)
  – confidentiality ok as long as the (current) settings are enforced
Further points for discussion

• Incentives of OSN providers wrt:
  – social privacy? surveillance? censorship?

• Is privacy always about information concealment (in social privacy / surveillance / censorship)?
  – Counter example: saying “I do not want to be disturbed”

• Censorship in PETs and in social privacy research
  – Privacy as establishing norms of respect vs. privacy as being able to break the norms

• Paradox of control
  – signaling that security is broken: false sense of security?

• Relationship (feedback) social privacy – surveillance
  – Surveillance -> social privacy problems: change of settings policies, bugs
  – Social privacy problems -> surveillance: what others reveal about you, social tagging improving identification of anonymous protesters
Conclusion

• Researchers in different subfields of CS frame the OSN privacy problem in very different ways
  – so does the media
• The different privacy problems are tackled as if they were completely unrelated
  – abstract away the complexity in order to reduce the problem to one that can be more easily addressed
  – some questions are left unaddressed
• We argue that the different privacy problems are entangled, rather than unrelated
  – a more holistic approach needed
  – integration of approaches extremely challenging