

• The challenge of protecting
privacy in the information era

Claudia Diaz

K.U.Leuven ESAT/SCD-COSIC

April 8 2011

About myself

- 2000: Master in Telecommunications Engineering (Telematics) from the University of Vigo (Spain)
 - 1999: Came to Leuven within the Erasmus program
- 2005: PhD in Engineering from the K.U.Leuven
 - PhD thesis: “Anonymity and Privacy in Electronic Services”
 - Information theoretic metrics for anonymity
 - Probabilistic analysis of anonymous communications systems
- Research on various aspects of privacy technologies
- October 2010: Assistant professor at K.U.Leuven ESAT/SCD-COSIC

What is privacy?

- Abstract and subjective concept
- Dependent on:
 - Cultural issues
 - Study discipline
 - Stakeholder
 - Context
 - ...
- We recognize privacy violations
- Hard to capture in a definition

(Non technical) privacy definitions (1)

- From a legal perspective
- “The right to be let alone” (Warren & Brandeis, 1890)
 - This citation was a response to technological developments, such as photography
 - Warren and Brandeis declared that information which was previously hidden and private could now be "shouted from the rooftops"

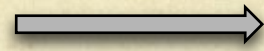
(Non technical) privacy definitions (2)

- “The right of the individual to decide what information about himself should be communicated to others and under what circumstances” (Westin, 1970)
- “Informational self-determination”
 - German constitutional ruling (1983)
 - “[...] in the context of modern data processing, **the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data** is encompassed by the general personal rights of the German Constitution. This basic right warrants in this respect the **capacity of the individual to determine in principle the disclosure and use of his/her personal data.**”

(Non technical) privacy definitions (3)

- From a social psychology perspective
- “The freedom from unreasonable constraints on the construction of one's own identity” (Agre and Rotenberg, 1998)
 - The construction of one's identity is always mediated by “gaze of the other”
 - Impression management / self-presentation
 - Social networks, profiling
- Intertwined with other concepts
 - Freedom, dignity, autonomy, (non-)discrimination, personal safety

Offline world



Online world

- Information is hard/costly to collect, store, search, and access
 - Conversation face-to-face
 - Letters in the post
 - Papers in an physical archive
 - Paying with cash
 - Following your movements
 - Knowing who your friends are
 - Looking for info in encyclopedia
 - Information hard to copy/disseminate, easy to destroy
 - Hard to aggregate, make profiles and inferences
 - Information forgotten after some time
 - ...
- Information is easy/cheap to collect, store search, and process
 - Skype, instant messaging
 - Emails
 - Files in digital archive
 - Paying with credit card
 - Location tracking
 - “Online” friends
 - Searching in google, wikipedia
 - Information easy to copy/disseminate, but hard to destroy
 - Easy to aggregate, make profiles and inferences: unique identifiers
 - Information never forgotten
 - ...

Nothing to hide?

- Solove: “The problem with the ‘nothing to hide’ argument is its underlying assumption that privacy is about hiding bad things.”
- “Part of what makes a society a good place in which to live is the extent to which it allows people freedom from the intrusiveness of others. A society without privacy protection would be suffocation.”
- Difference between “secret” and “private”
 - Your daily routine, your movements, who your friends are, what you said in a conversation, which books you read...
 - This may not be secret, but you may not be comfortable with making it public or having external entities knowing about it, analyzing it, and extracting conclusions from it



PLEASE ROB ME



Raising awareness about over-sharing

Check out our [guest blog post](#) on the CDT website.



Next step



We are satisfied with the attention we've gotten for an issue that we deeply care about. If you're interested, you might like to read these articles:

- [On Locational Privacy, and How to Avoid Losing it Forever](#)
- [Over-sharing and Location Awareness](#)

More Info

[Home](#)

[Why](#)

Made Possible By

[Foursquare](#)

Privacy and technology

- Bottom line: our actions and interactions are increasingly mediated by technology
 - We leave digital traces everywhere
 - Traces are combined, aggregated, and analyzed to infer further information about ourselves and to make decisions that affect us
 - We have no control over our information, or the inferences derived from it (lack of transparency)
- Information is never forgotten
 - But will perhaps be taken out of context

Privacy Enhancing Technologies (1)

- Legal protections are necessary but not sufficient
- It is not about switching off all electronic devices!
 - We want to enjoy the advantages of new ICTs while maintaining as much as possible the degree of privacy we enjoy in the offline world
- Cryptography
 - Encryption to protect content
 - Privacy-preserving cryptographic protocols
 - Anonymous authentication
 - Private set intersection
 - Oblivious transfer
 - ...

Privacy Enhancing Technologies (2)

- Database privacy
 - Differential privacy
 - Possible to extract statistical information from databases without compromising the privacy of the individuals whose data is in the database
- Access control
 - Policies that define who can access what information
 - Enforcement mechanisms
 - Privacy settings

Privacy Enhancing Technologies (3)

- Privacy is not only about information explicitly provided
 - Gives vs. give-offs: e.g., what you say vs. your body language
- Traffic data
 - Who communicates with whom, when, from where, for how long, how frequently, what is accessed, ...
 - Machine-readable + low volume: very easy to process
- Traffic analysis: techniques to analyze traffic data and extract information from it
 - Provides information on intentions and activities, status in your social circle, location tracking, etc.
 - Probabilistic methods: contrast with classical security analysis such as cryptanalysis, provable security, access control

Traffic analysis

- Example 1: Gaydar
 - What others reveal about you
 - Challenges informational self-determination (“my” data) and DP concept of “consent”
 - Another example: DNA data
- Example 2: LinkedIn
 - Rate of creation of links between employees of company A and B may indicate an imminent merger or a new business relationship
- Example 3: Location tracking
 - Reveals: religion, health information, daily routines, etc.

FACEBOOK DIGG STUMBLEUPON REDDIT PRINT

Gaydar Algorithm Outs Facebook Users

By Susannah F. Locke Posted 09.21.2009 at 12:27 pm 9 Comments



THE SEX FILES

What are your friends saying about you? Online social networks like this Facebook one might reveal more about you than you think [Juvetson](#) (CC licensed)

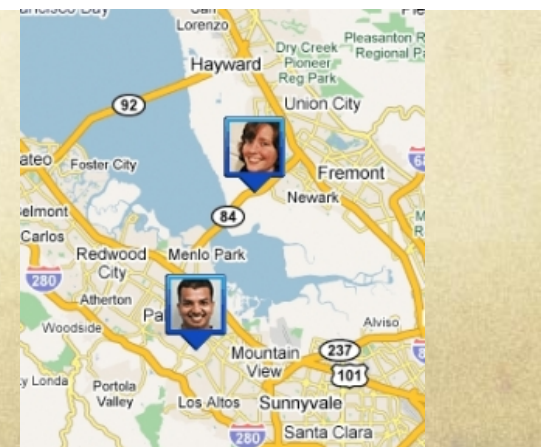
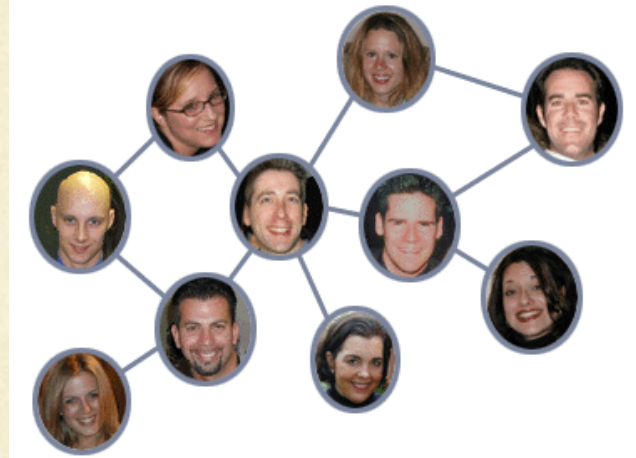
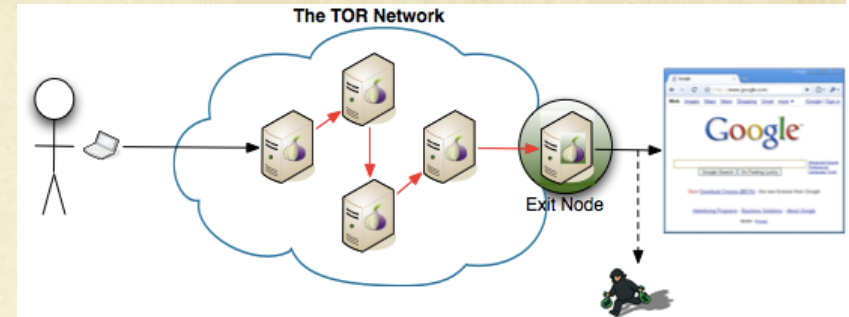
A pair of MIT students claim that they have created an algorithm that outs gay members of Facebook by analyzing the sexual orientations of their networks of friends.

Research challenges

- How to translate the abstract concept of privacy into technical properties
 - Classical security: confidentiality, integrity, authentication, availability
 - Privacy: anonymity, unlinkability, unobservability, deniability (OTR)
- How to measure the extent to which these properties are satisfied in a system
 - Privacy metrics
- How to analyze privacy systems
 - Current analysis techniques too ad-hoc
 - General analysis methodologies
- How to design privacy systems
 - Compositionality of privacy technologies
 - Privacy-by-design methodologies

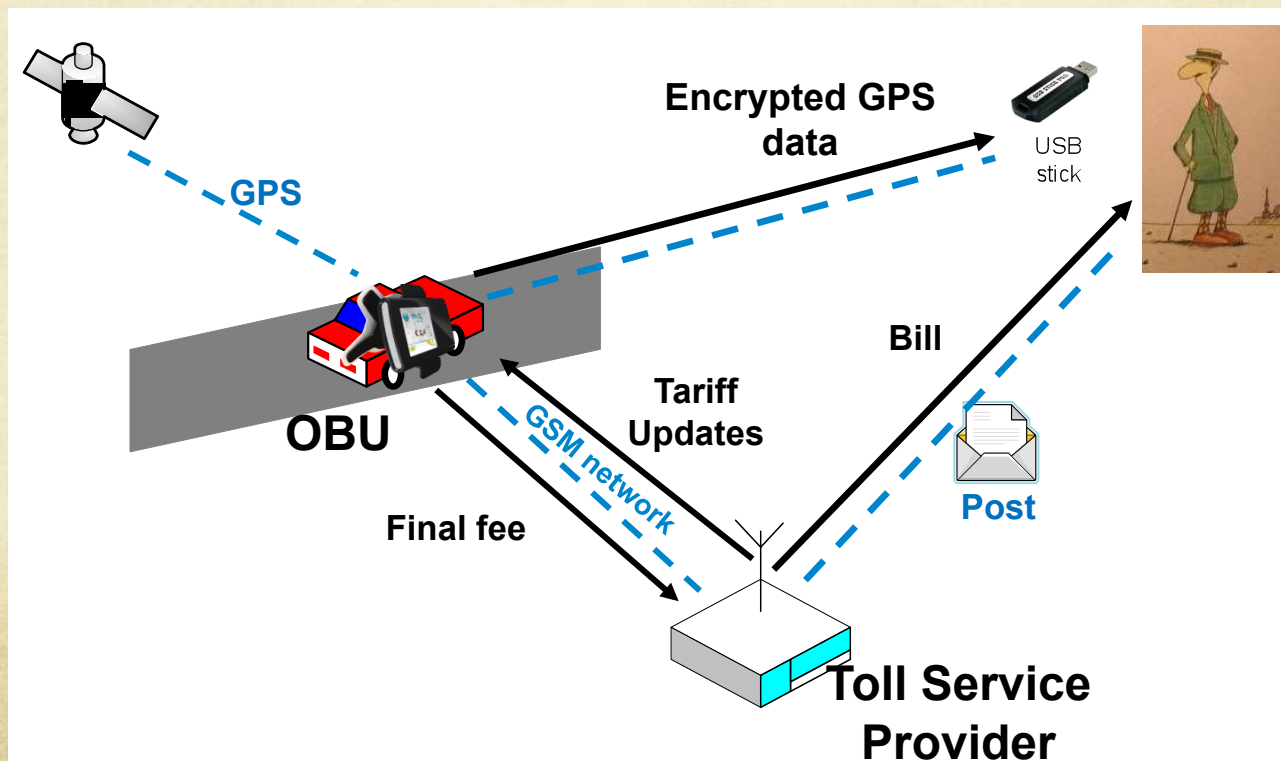
Applications

- Communication infrastructure
 - Anonymous and unobservable communications
 - Wide range of systems: email, web browsing, instant messaging, voice over IP, etc.
- Social networks
 - Content and traffic data (friendship links, interactions, information flow)
 - Better understanding of privacy risks, propose solutions
- Location privacy
 - Wide range of systems: mobile applications, vehicular applications, ambient intelligence, road pricing
- Other: smart metering, e-health, identity management, ...



Privacy Enhanced Road Tolling

- Personal data kept in the user device (not in backend database)
- Detects cheating and ensures correct payments while preventing location tracking



Projects

- Social networks
 - IWT SBO project (from Jan 2011)
 - Improve privacy protection in social networks
 - Interdisciplinary: technology (KULeuven ESAT/COSIC, CS/Distrinet, CS/DTAI), law (KULeuven ICRI), economics (CMU), social aspects (VUB), educational aspects (Ugent)
- Location privacy
 - FWO project (from Jan 2011)
 - Develop conceptual, ethical, and analytical framework for location privacy
 - Interdisciplinary: technology (KULeuven ESAT/COSIC) and law/ethics/human rights/philosophy (VUB LSTS)

Conclusions (1)

- ICT developments have changed the game for privacy
 - Profound implications for our society and democracy
 - Asymmetry of information leads to changes in the balance of power
 - How we resolve privacy issues will be crucial for defining the type of society we live in
- Shared infrastructures
 - An infrastructure that leaks private information affects not only individuals, but also businesses and governments
 - “Communication is fundamental to our species; private communication is fundamental to both our national security and our democracy.” (Diffie and Landau)

Conclusions (2)

- Incredibly challenging and exciting topic to work on
 - Nuanced and complex topic not only technically, but also conceptually
 - Strongly interdisciplinary: technology, law, sociology, ethics, ... essential to understand the bigger picture
 - Communicate with policymakers, civil liberties activists, industry
- Education
 - Need for educating students in the privacy risks and solutions
 - As individuals and as professionals

Thank you!



<http://homes.esat.kuleuven.be/~cdiaz/>

claudia.diaz@esat.kuleuven.be