UNIVERSITÉ CÔTE D'AZUR

Inria INVENTEURS DU MONDE NUMÉRIQUE

01. Introduction to Privacy and Course organization

Nataliia Bielova

@nataliabielova

September 17th, 2018

Web Privacy course

University of Trento

Today's class

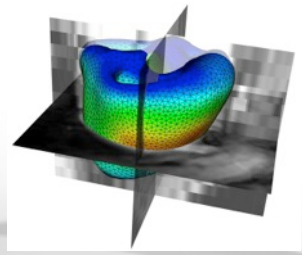
- Course staff introduction
- Privacy = ???
- Overview of course topics
- Student introductions

Who am I

- **Nataliia Bielova**, PhD 2011
  - nataliia.bielova@inria.fr
- **Research scientist at Inria,** the French National Institute in computer science and automation
- **Interests**
  - Privacy protection
  - Web Tracking technologies
  - Discrimination on the Web
  - EU Privacy law enforcement

Science at Inria

MODELS
AND SIMULATION



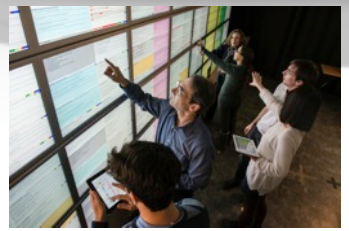
HIGH-PERFORMANCE
COMPUTING, CLOUD

NETWORKS AND
CONNECTED
OBJECTS

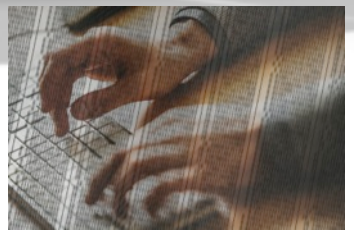
SAFETY,
RELIABILITY

ROBOTICS

PROGRAMMING

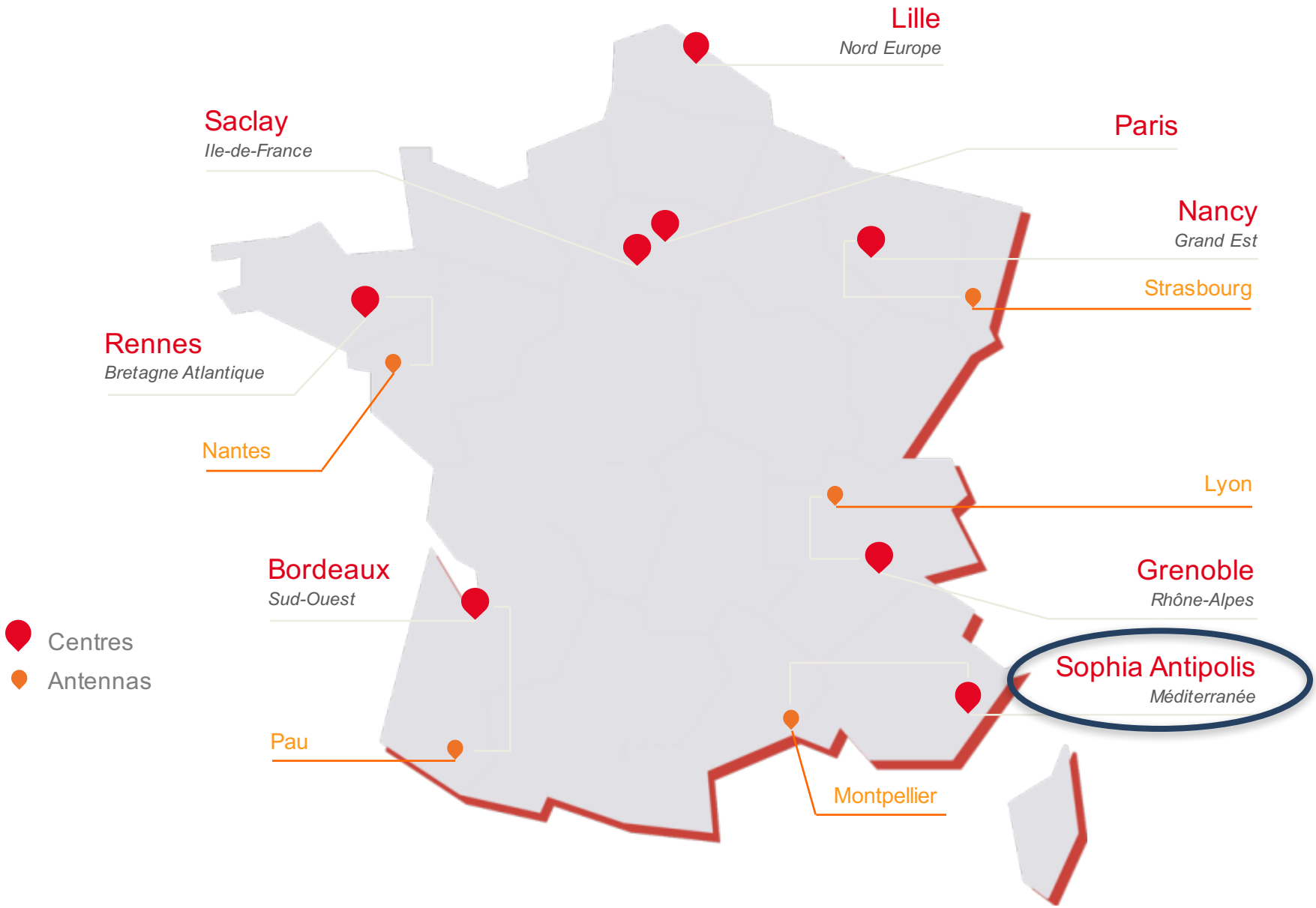


INTERACTIONS,
INTERFACES AND
USAGE

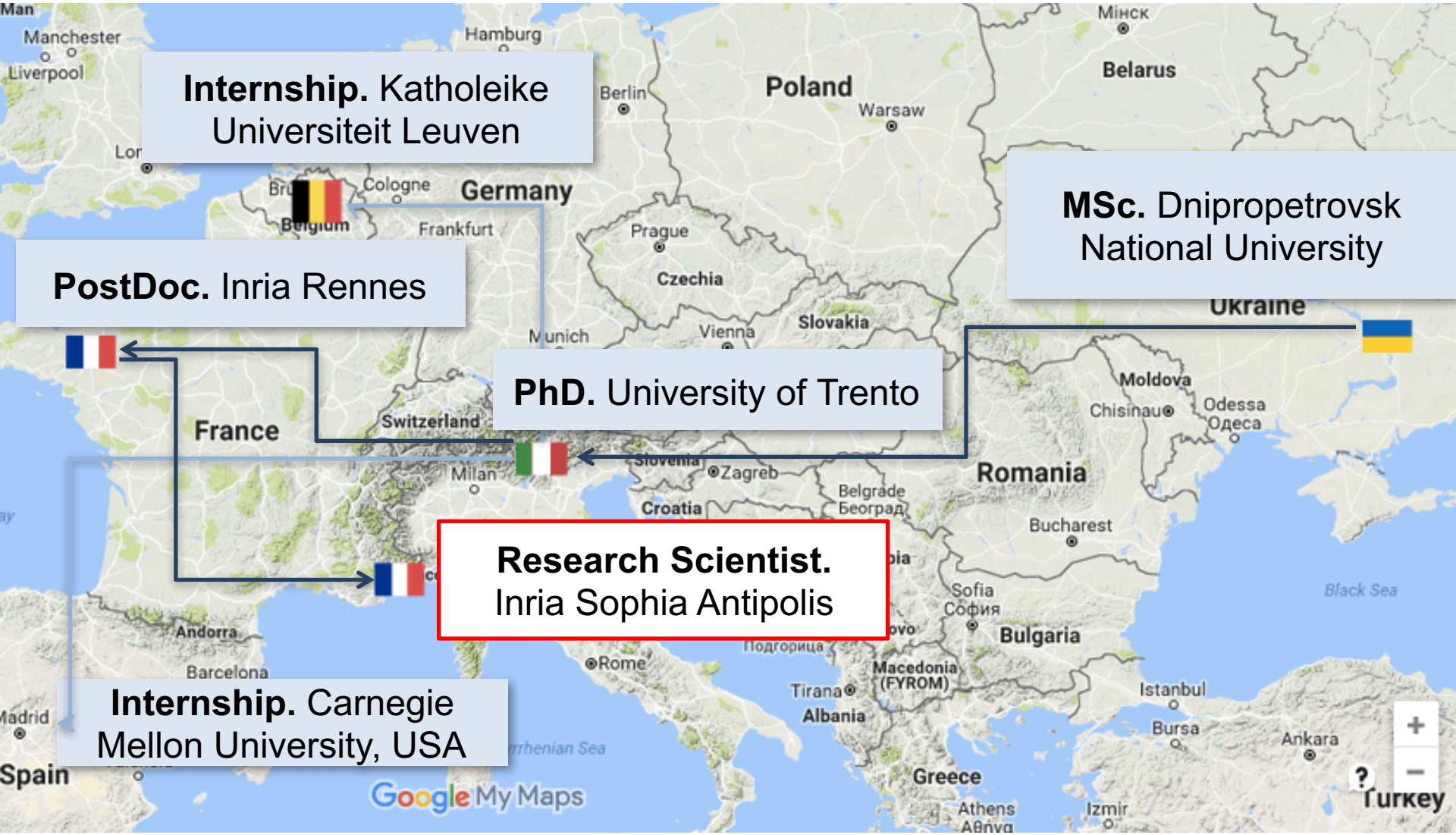


DATA
PROCESSING

Research centres



My career path to Inria



What is Privacy?

Back in 1993…

"On the Internet, nobody knows you're a dog."

Today…

It's the Internet! Of course they know you're a dog. They also know your favorite brand of pet food and the name of the cute poodle at the park that you have a crush on!

What is privacy?

- Your answers!

What is privacy?

- Abstract and subjective concept

- Depends on
  - Study discipline
  - Social norms and expectations
  - Context

From slides of Claudia Diaz

1890*

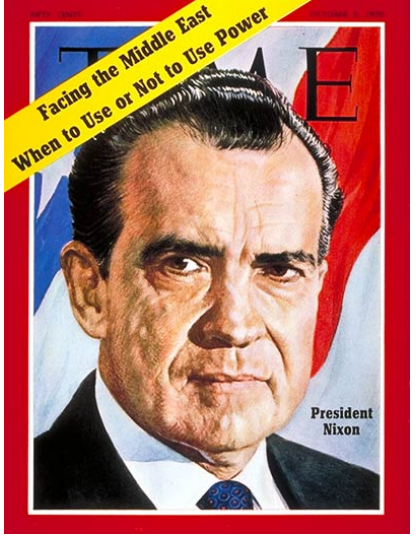
"The right to be let alone"

Warren & Brandeis (1890)

*The first advertising agency was established in 1890 as well!

From slides of Claudia Diaz

1970



"The right of the individual to decide what information about himself should be communicated to others and under what circumstances"

Westin (1970)

From slides of Claudia Diaz

1978

- Definition of “personal data “: any informaiton relating to an individual
- “It’s prohibited to collect and process personal data from racial, ethnic, political, philosophical or religious type, and data related to health or sexual orientation”

Privacy and informatics law, France

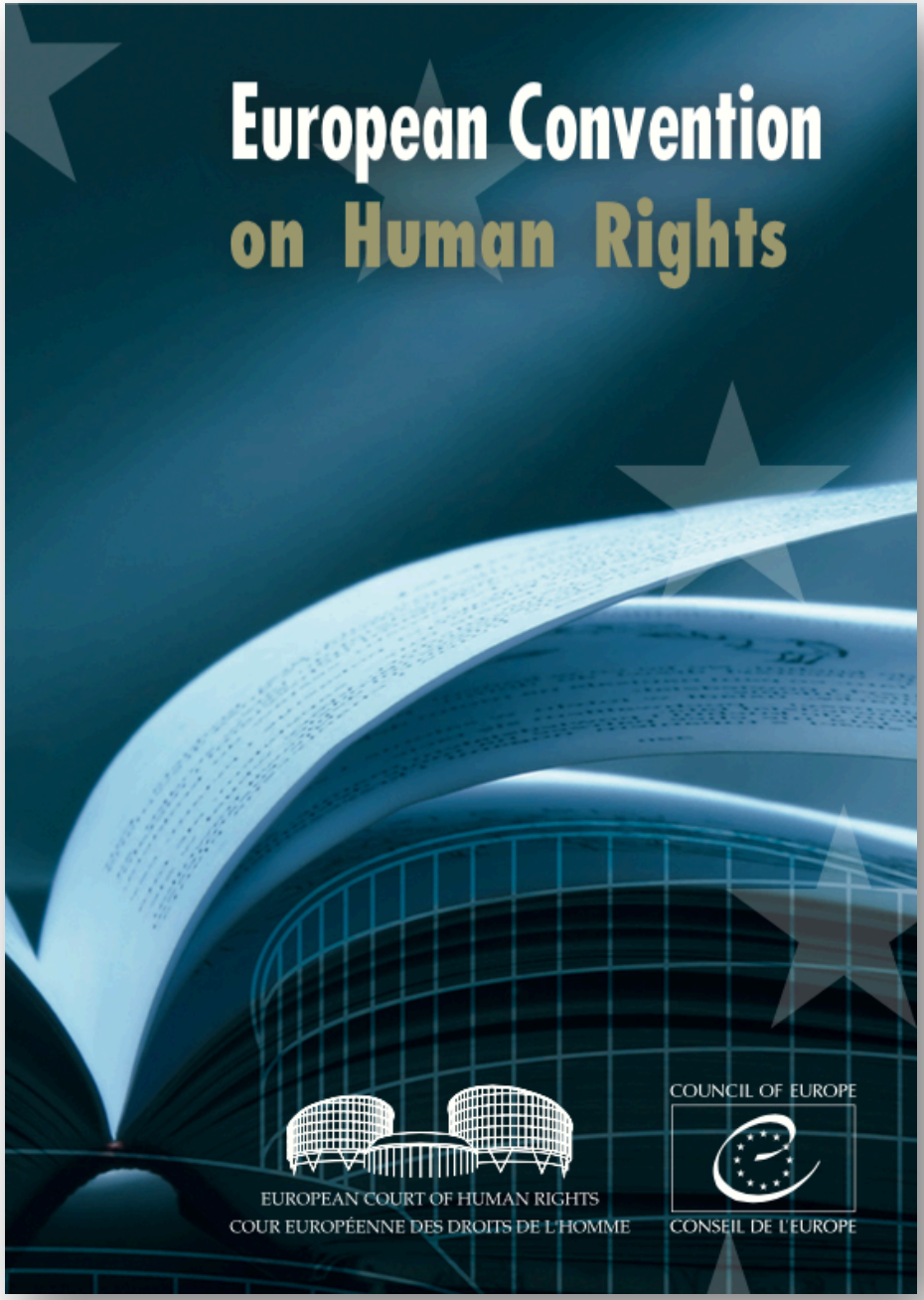
“Loi informatique et liberte” (1978)

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**."

"Informational self-determination"
German constitutional ruling (1983)

From slides of Claudia Diaz


European Convention
on Human Rights
EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

1953

European Convention on Human Rights

- Emerged as a response to the excesses of totalitarian states in the 30s and 40s (entered into force in 1953)
  - Spirit: protect **citizens** from an overbearing/intrusive **state**
  - During the cold war: 'western' states would distinguish themselves from the 'eastern block' in that the population was not subject to pervasive surveillance

From slides of Claudia Diaz

European Convention on Human Rights

Article 8 – *Right to respect for private and family life*

1. **Everyone** has the **right** to respect for his private and family life, his ***home*** and his ***correspondence***.
2. There shall be no interference by a public authority with the exercise of this right **except**
   - such as is in accordance with the law and is necessary in a democratic society in the interests of ***national security***, ***public safety*** or the ***economic well-being of the country***, for the ***prevention of disorder or crime***, for *the* ***protection of health or morals***, or for the protection of the rights and freedoms of others.

From slides of Claudia Diaz

Data Protection

- EU Data Protection Directive (1995)
- General Data Protection Regulation, GDPR (2018)

- Defines and applies to “Personal data”

- What is “**Personal data**”?
  - → see slides of Vincent Roca

From slides of Claudia Diaz

Data Protection Principles

- **Transparency**
  - Informed consent of the data subject, access rights
  - Necessity based on contractual, compliance, public interest, etc.
- **Legitimate purpose**
  - Personal data can *only* be processed for specified explicit and legitimate purposes, purpose limitation
- **Proportionality**
  - Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed (aka “data minimization”)
- **Accountability** of the data controller

From slides of Claudia Diaz

Related concepts

- Intertwined with other concepts
  - Freedom: anonymous speech, freedom of association
  - Dignity: airport scanners
  - Autonomy: censorship, filter bubble
  - (Non-)discrimination: profiling and personalization
  - Personal safety: identity theft
  - Democracy: targeted political messaging exploiting psychological biases

From slides of Claudia Diaz

Privacy and Technology

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
- Easy to copy/disseminate, but hard to destroy
- Easy to aggregate, make profiles and inferences: unique identifiers
- Information never forgotten
- …

From slides of Claudia Diaz

2003

"Privacy management is *not about setting rules and enforcing them*; rather, it is the **continual management of boundaries** between different spheres of action and degrees of disclosure within those spheres. **Boundaries move dynamically as the context changes**. These boundaries reflect tensions between conflicting goals; boundaries occur at points of balance and resolution. "

Unpacking "Privacy" for a Networked World
Palen & Dourish

But I've got nothing to hide!

Do you still agree? Why?

But I've got nothing to hide!

- If you are still convinced…
  - So do you have curtains?
  - Can I see your credit card bills for the last year?
  - I don't have anything to hide. But I don't have anything I feel like showing you, either.
  - **Show me yours and I'll show you mine.** Exercise!
  - It's not about having anything to hide, it's about things not being anyone else's business.

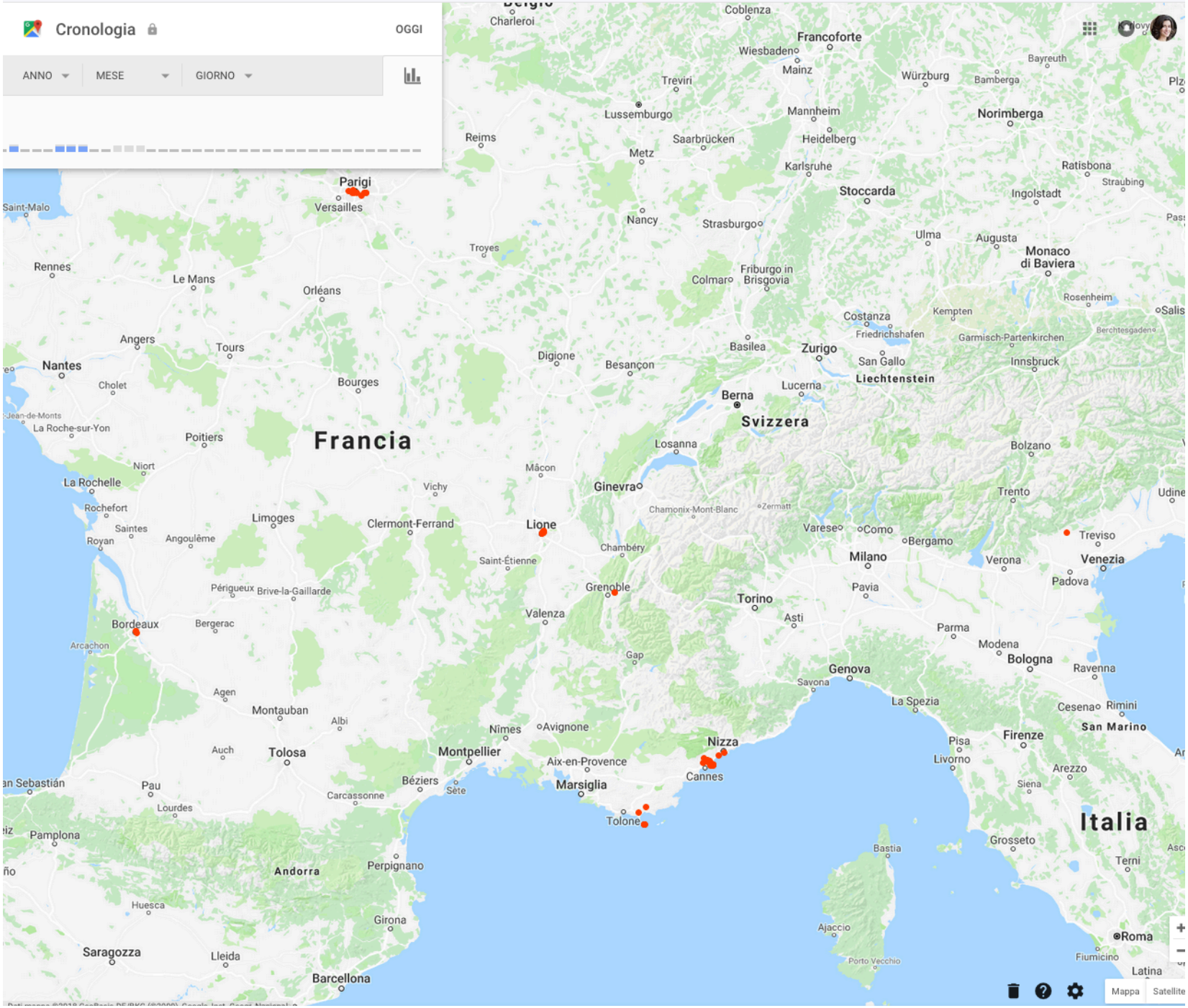
D. Solove (2007)

Exercise!

Exercise 1: Your location

- Google stores your location (if you have it turned on) every time you turn on your phone, and you can see a timeline from the first day you started using Google on your phone
- Open your Google location history:
  - https://www.google.com/maps/timeline?pb

- Show it to the colleague on your right!
  - Does (s)he guess where do you live?
  - What did you do last summer?


Cronologia
OGGI
ANNO
MESE
GIORNO
Francia
Svizzera
Italia
Liechtenstein
Parigi
Versailles
Lione
Ginevra
Nizza
Cannes
Marsiglia
Tolone
Montpellier
Bordeaux
Milano
Torino
Genova
Venezia
Zurigo
Berna
Basilea
Strasburgo
Francoforte
Stoccarda
Norimberga
Monaco di Baviera
Andorra
Barcellona
Saragozza
Roma
Mappa
Satellite

Exercise!

Exercise 2: Your activity

- Google stores search history across all your devices on a separate database
- Open your Google activity:
  - https://myactivity.google.com/myactivity

- Show it to the colleague on your left!
- Are you still OK to show it?

Exercise!

More exercises for Google

- Show these to your neighbor:
  - Google advertisement profile:
    - http://www.google.com/settings/ads/
  - App and extension info:
    - https://myaccount.google.com/permissions
  - Youtube history:
    - https://www.youtube.com/feed/history/search_history

- All the data Google stores about you:
  - https://takeout.google.com/settings/takeout

Not a Google user? Download and show your Facebook data then!

- https://www.facebook.com/help/1701730696756992?helpref=hc_global_nav

I've got nothing to hide!

- "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**."

D. Solove (2007)

From slides of Claudia Diaz

I've got nothing to hide!

- Difference between "secret" and "private"
  - Your daily routine, your movements, who your friends are, what you said in a conversation, which books you read...
  - These 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

From slides of Claudia Diaz

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 used out of context

From slides of Claudia Diaz

Privacy Technologies

- Aim to address / mitigate certain privacy concerns
  - While allowing us to enjoy the benefits of the modern ICTs

Web Privacy

Course organization

Logistics

- Updated syllabus is always available on the course web page:
  - http://www-sop.inria.fr/members/Nataliia.Bielova/teaching/wp2018
- Alternatively, choose
  - Nataliia's webpage → Teaching → Web Privacy

Evaluation

- Choose one topic of the course
- Write a review of 2 papers related to this topic
- Papers available on the course webpage

- Submit your review
  - Subject: [WebPrivacy2018] NAME SURNAME
  - Email: nataliia.bielova@inria.fr

- Deadline: **5 October 2018**

Course topics

- Introduction to Privacy, Web applications and economic model of the Web.
  - How to use various browser technologies to track users on the Web?
  - How to design privacy-compliant Web applications?
  - How to protect your own privacy online?
  - Why do I see relevant ads? How targeted advertisement works?
  - How laws cover Web and mobile applications?
  - Is there privacy in social networks?

Topic 1: Web Tracking technologies: Cookies

- Web Tracking technologies intro
- Within- and cross-site tracking: what's the difference?
- Tracking via cookies and other stateful technologies
- Cookie resurrection aka zombie cookies

Topic 2: Web Tracking technologies: Browser fingerprinting

- A brief history of Web browsers
- Browser fingerprinting definition
- From basic to advanced fingerprinting
- Detecting evolution of fingerprints
- Device fingerprinting

Topic 3: Protection from Web Tracking

- Browser settings – are they effective?
- Private or incognito mode
- AdBlock and other ad blocking tools – do they protect from tracking?
- Tracking blocking tools
- Protection from browser fingerprinting

Topic 4: Privacy in Targeted advertising and Ads explanations

- Targeted advertising
- Real-Time Bidding protocol (RTB)
- Cookie synching
- Attribute and PII-based targeting on Facebook
- Investigating Facebook Ad explanations

Topic 5: Smartphone privacy

- Why do smartphones interest so many people?
- Free apps/services in exchange of targeted advertising: where's the problem?
- What is personal in my smartphone: a close-up on technical identifiers
- User control
- Limits of the user control
- Two further examples: ACCESS_WIFI_STATE and physical world tracking

Topic 6: Privacy policies and human aspects of Privacy

- **How easy is to read and understand** privacy policies?
- **Notice and choice** mechanism: how effective is it?
- Measurement of privacy policies, notice and choice
- **Concise formats** to show policies
  - **Tools to extract information** from human-readable policies

Topic 7: Privacy in social networks

- Privacy concerns in SNSs
- Measuring privacy perceptions in SNSs
- “Social privacy” controls and practices
- Privacy nudges
- Privacy paradox