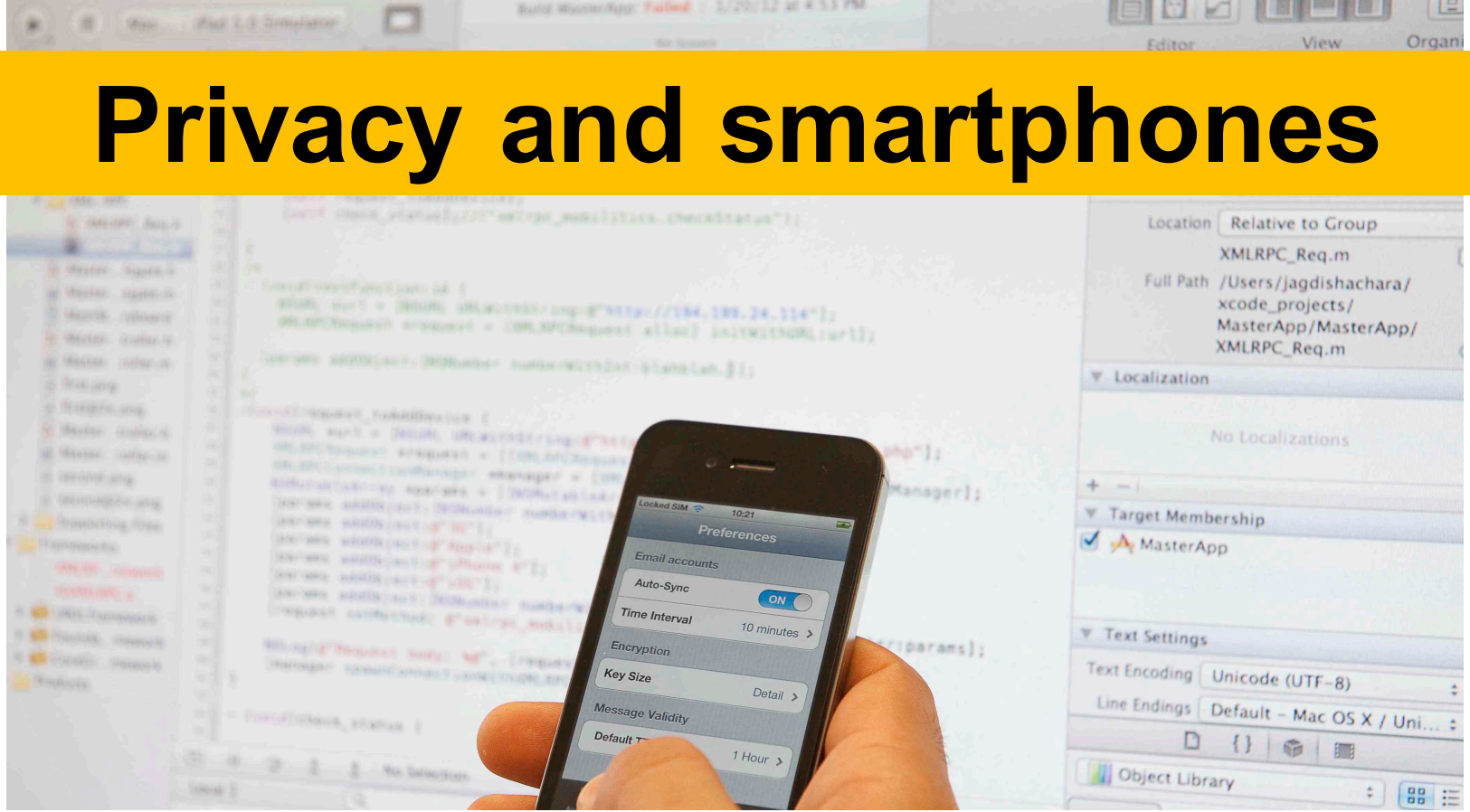
Privacy and smartphones



Vincent Roca, Inria PRIVATICS, vincent.roca@inria.fr

informatiques mathématiques
Inria

contact : vincent.roca@inria.fr

Outline

- Personal data and the French/EU law
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- 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
- Conclusion: towards a virtuous circle

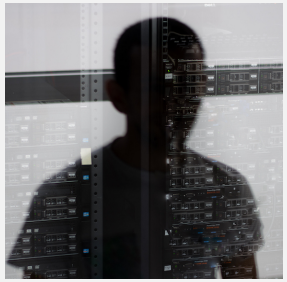
Outline

- **Personal data and the French/EU law**
- Context: a massive worldwide surveillance
- Why do smartphones interest so many people?
- The ecosystem around applications for smartphones
- 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
- Conclusion: towards a virtuous circle

Some vocabulary…

Private company, administration
"data controller"
(responsable de traitements)

has the responsibility of



Data Base containing
"Personal Information"
(données à caractère personnel)

relative to

Physical persons

We'll talk about…

Personal and sensitive information definition in FR/EU

↓

Other viewpoints

↓

Associated obligations for the data controller

↓

PI transmission outside of EU

↓

Official ways to escape the PI rules

Personal information according to the “Loi informatique et libertés” of 1978 (1)

identity is not required as long as a path to an identity can be found

Article 2 : […] Constitue une donnée à caractère personnel toute information relative à une **personne physique identifiée ou qui peut être identifiée, directement ou indirectement**, par référence à un numéro d’identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de **considérer l’ensemble des moyens** en vue de permettre son identification dont dispose ou auxquels peut avoir accès le **responsable du traitement ou toute autre personne.** […]

http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

no limit on the technical means

no limit: anybody in the world

Personal information according to the “Loi informatique et libertés” of 1978 (2)

- the **nature** of the information does not matter…
  - ✓ can be anything (e.g., temperature in a home)
- …if there is a **link to a person**, it’s a Personal Info (PI)

- this link can be **direct**…
  - ✓ e.g., we record temperature + name
- or **indirect**
  - ✓ e.g., we record temperature + EDF client ID

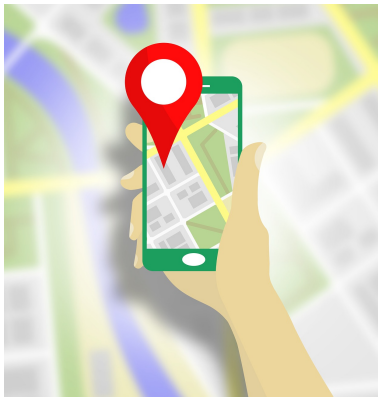
Personal information according to the “Loi informatique et libertés” of 1978 (3)

- a person is considered **identifiable** if the data controller has the information to identify him
  - ✓ e.g., EDF collects your home temperature + EDF client ID
- or **anybody else** in the world
  - ✓ e.g., EDF collects your home temperature + IP address of the sensor.
  - ✓ Here the ISP can link the IP to the ADSL user

- NB: a commonly used term, **PII (Personally Identifiable Information)**

The particular case of “sensitive information” (2)

- Sensitive information cannot be collected and processed (except in a few particular cases).
  - ✓ The “Loi Informatique et Libertés” lists a few exceptions
  - ✓ ex. Health professionals and medical urgencies



- What about “**inferences**”?
  - ✓ in practice it’s pretty complex because of inference
  - ✓ if Google knows I’m at a church every Sunday morning (thanks to geolocation) he knows something whose collection is prohibited

Other viewpoints on personal information (1)

- The FR (and European) definition of PI is very protective☺

- In certain countries, the link between data and physical person is only considered for the **data controller**
  - ✓ Changes everything!
  - ✓ *e.g., if X collects "temperature + IP address of the sensor », data is not considered as PI unless X is an ISP…*

Other viewpoints on personal information (2)

- Question 1: what about the following claim?

  “we don’t collect your name, age or address, only non personal information”

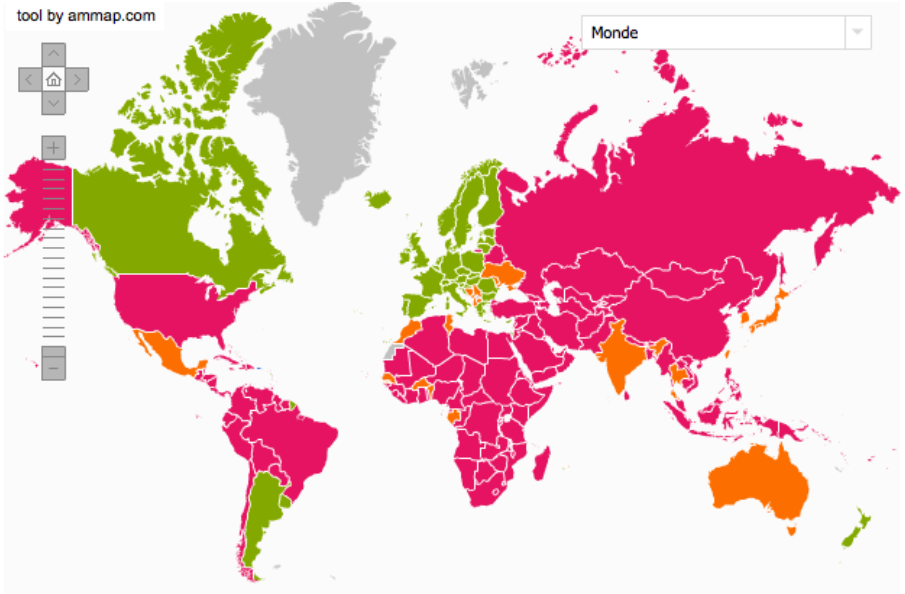
  - ✓ wrong if linkability to a person remains possible

- Question 2: is an IP address a PI?
  - ✓ yes in France and in EU
  - ✓ no in the US, apart from the ISP

PI transmission beyond EU (1)

- Personal information of EU citizens **cannot** be sent beyond EU borders.

- **Solution 1:** there are exceptions for countries whose data protection law is compliant with that of EU



https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

PI transmission beyond EU (2)

- US is not concerned by this exception
  - ✓ US is not recognized as trustworthy W.R.T. PI protection

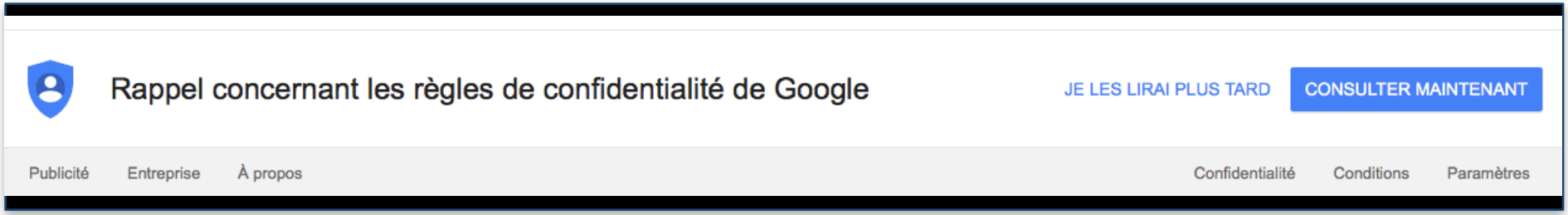
- **Solution 2:** join the **Privacy Shield** program that rules PI transfers to the US
  - ✓ The company commits to respect the contractual obligations
  - ✓ A previous program, “Safe Harbor”, has been canceled in 2015 by the EU Court of Justice: see the EUJC judgment (Max Schrems)

https://www.cnil.fr/fr/le-privacy-shield
http://www.cnil.fr/linstitution/actualite/article/article/invalidation-du-safe-harbor-par-la-cour-de-justice-de-lunion-europeenne-une-decision-cl/

Ways to escape the PI rules (1)

The data collector can do much more if…

- **Solution 1:** he obtains the **“free and informed consent”** of the user
  - ✓ “consentement libre et éclairé”
  - ✓ explains why Google urges the user to read their confidentiality rules



- is it sufficient?
  - ✓ no if the user is not free to use the service (no alternative)
  - ✓ no if the privacy rules are not compliant with French / EU law (ex. Facebook)

Ways to escape the PI rules (2)

- **Solution 2:** data is **anonymized**
  - if linkability to a person is impossible it is no longer PI
  - but secure anonymization can be pretty hard to achieve and not necessarily sufficient
    - ✓ because of **inference attacks with side information**
    - ✓ e.g., if a group of people is known to have a certain property, and if I'm known to belong to this group, even if my individual record cannot be identified in the database, one knows I have this property too

To summarize

- Notions of personal information and sensitive information:
  - ✓ are the foundation of laws that protect privacy
- A data controller that owns PI must comply with several key obligations.
- PI transmission beyond EU is possible but laws exist that protect it.
- In order to escape these obligations:
  - ✓ get the “free and informed consent” of the users;
  - ✓ anonymize the database.

Ressources

CNIL. « Loi informatique et libertés » de 1978 :

http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

CNIL. Protection des données dans le monde : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

CNIL. Privacy Shield : https://www.cnil.fr/fr/le-privacy-shield