Anonymity and Privacy

Ivan Marin
Daitan Group
imarin@daitangroup.com

Anonymity and Privacy

Concerns about the anonymity and privacy of the data used on Machine Learning Models

Summary

- What is privacy
- “I have nothing to hide!”
- Privacy in ML models
- Privacy in Healthcare
- Anonymity

Why?

First of all, I’m no expert in privacy.

I had to learn about it by pure need!

Does anyone here has experience with privacy?

What is privacy

“*Privacy* is the ability of an individual or group to seclude themselves, or

information about themselves,

and thereby express themselves selectively.”

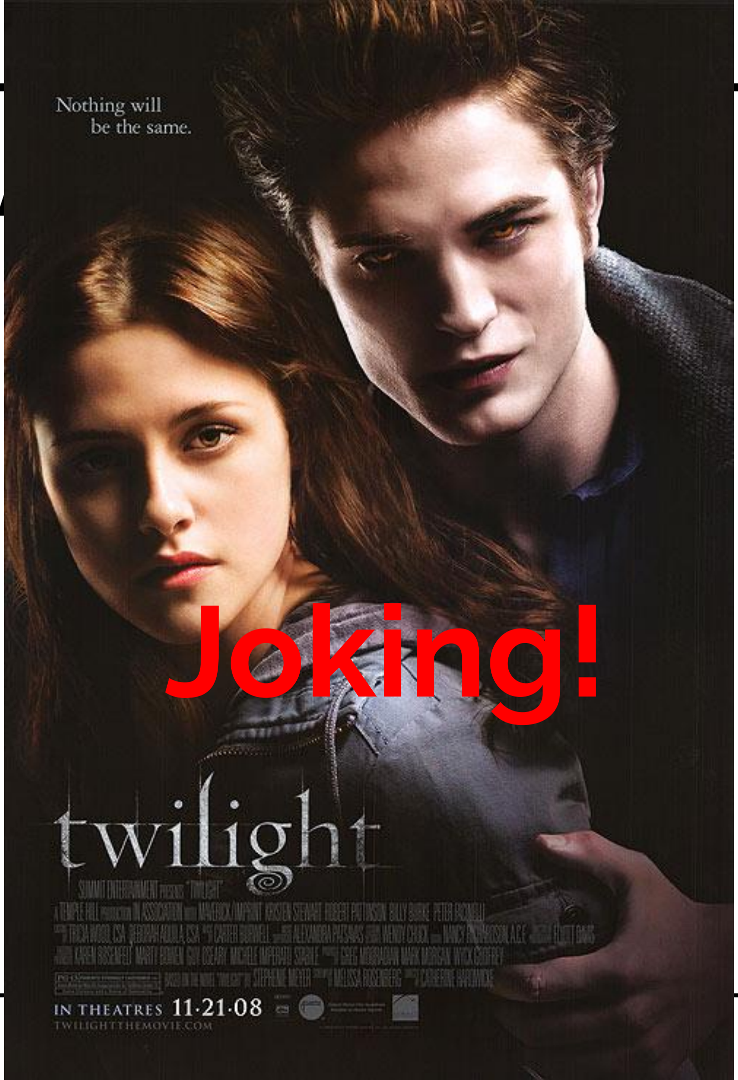
Privacy

It means the power to select what to share and with whom.

- It's not absolute
- It varies by culture
- It varies by time period
- Can be limited by law (taxes)

“I have nothing to hide!”

“I hav


Nothing will
be the same.
twilight
IN THEATRES 11·21·08
TWILIGHTTHEMOVIE.COM

Joking!

“I have nothing to hide!”

- Public registry of Amsterdam population since the 1880s, including *religion*
- Medical records
- Attorney conversations
- What you´ve purchased last month, last year

Personally Identifiable Information

“Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.”

https://en.wikipedia.org/wiki/Personally_identifiable_information

Personally Identifiable Information

Depends on context, but in general can be:

- Full name
- Face (image)
- Home address
- email address
- National identification number
- Fingerprints
- Date of birth
- Age, gender, color ...

Personally Identifiable Information

Should it be protected? Common questions:

- How is this data captured?
- Who holds this data?
- Who can access this data?
- For how long will this data be stored?
- Will this data be shared?

Privacy: Collection and use

Collection and use are different things

- What is not collected cannot be used
- What is not collected (usually) cannot be collected later
- What is not collected cannot be leaked

So what can be used? What are the **rules**?

Privacy in ML

- What data can you use in your model?
- Do you know if you can use it?
- How models can be biased?

Privacy in ML - Biased models

A ML model can be biased given the data distribution that it was trained

- Credit scoring that allows loans
- Prison sentencing models that can make people spend more time in jail because of racial differences

What data can you use in your model?

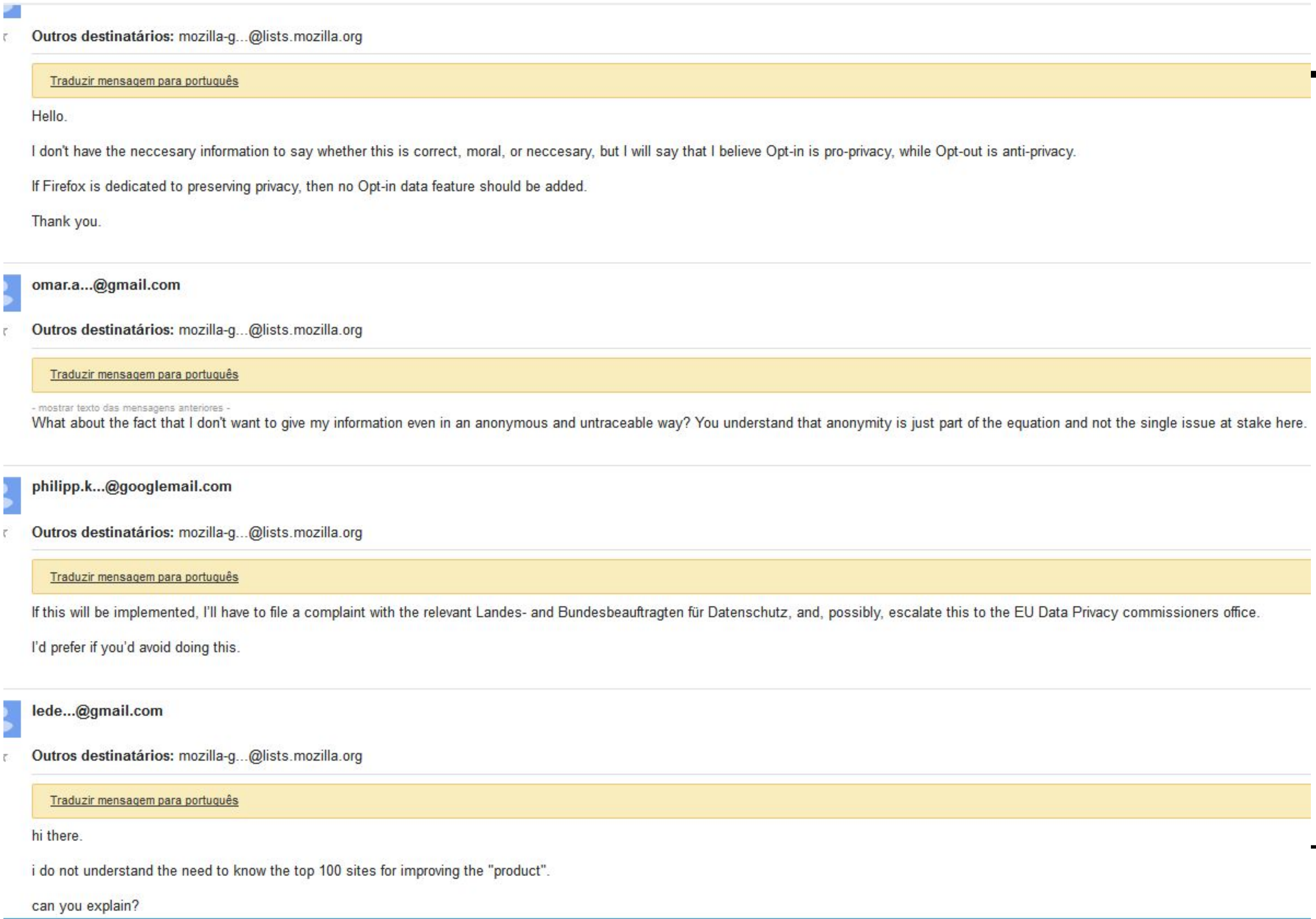
Opt-in versus Opt-out: *Consent*

Devs at Mozilla are proposing to collect more information about its users to improve crash reports in Firefox

But instead of Opt-in they're arguing to be opt-out.

https://groups.google.com/forum/#!topic/mozilla.governance/81gMQeMEL0w

https://news.ycombinator.com/item?id=15071492



Outros destinatários: mozilla-g...@lists.mozilla.org

Traduzir mensagem para português

Hello.

I don't have the neccesary information to say whether this is correct, moral, or neccesary, but I will say that I believe Opt-in is pro-privacy, while Opt-out is anti-privacy.

If Firefox is dedicated to preserving privacy, then no Opt-in data feature should be added.

Thank you.

omar.a...@gmail.com

Outros destinatários: mozilla-g...@lists.mozilla.org

Traduzir mensagem para português

- mostrar texto das mensagens anteriores -

What about the fact that I don't want to give my information even in an anonymous and untraceable way? You understand that anonymity is just part of the equation and not the single issue at stake here.

philipp.k...@googlemail.com

Outros destinatários: mozilla-g...@lists.mozilla.org

Traduzir mensagem para português

If this will be implemented, I'll have to file a complaint with the relevant Landes- and Bundesbeauftragten für Datenschutz, and, possibly, escalate this to the EU Data Privacy commissioners office.

I'd prefer if you'd avoid doing this.

lede...@gmail.com

Outros destinatários: mozilla-g...@lists.mozilla.org

Traduzir mensagem para português

hi there.

i do not understand the need to know the top 100 sites for improving the "product".

can you explain?

What data can you use in your model?

What kind of data do you need for your model?

- Relevant variables versus privacy
- Real name versus identifier
- Real numbers versus shifted numbers

Privacy in Healthcare

- HIPAA: Health Insurance Portability and Accessibility Act (1996)
- PHI: Protected Health Information
  - Can be used in Research, subject to restrictions
- 18 data categories that **must** be removed
  - Name
  - Geographical identifiers
  - Dates, including birth dates
  - etc…

http://cphs.berkeley.edu/hipaa/hipaa18.html

Privacy in Healthcare

- Even after removing the required information, some fields need to be **obfuscated** or **hashed**
- The data cannot be shared by the researcher to any other party
- The data must be retained for 6 years after the end of the research project

Privacy in Healthcare: Example

Data Source: Electronic medical records platform

- Input Fields:
    - Patient name
    - age
    - admission date
    - admission department
    - admission condition
    - treatment
    - physician
    - discharge date
    - discharge cause

Privacy in Healthcare: Example

Model objective: predict discharge rate

- Transformed fields:
    - Patient name: dropped
    - age: partitioned into 5 divisions
    - admission date: shifted by fixed number of months into the future
    - admission department: as is
    - admission condition: as is
    - treatment: dropped
    - physician id: hashed by SHA265 + salt
    - discharge date: shifted by a fixed number of months into the future
    - discharge cause: as is

Privacy in Healthcare: Example

Results: Linear regression

- Reasonable agreement with training data
- Bad performance on test data
- … Overfitting

Privacy in Healthcare: Example

Results: Time series

- Reasonable agreement with training data
- Reasonable performance on test data
- … Only aggregated at Hospital level

Privacy in Healthcare

Could the model be improved? But on what cost?

Tradeoff between prediction benefits and patient privacy must be taken into account.

Privacy: loss of privacy

What could happen if the healthcare dataset was leaked?

- An attacker could get the entrance and exit date, ballpark age and condition/department
- With a bit more information (an employer e.g.), the person could be identified by the behavior pattern

So to respect privacy sometimes one has to also guarantee **anonymity**

Anonymity

“The idea (...) that a person be

non-identifiable, unreachable, or untrackable.”

Anonymity

It means that any action done by a person cannot be related, identified or connected to that person.

- It can be enforced by law (elections)
- Can be prevented by law (Brazil)
- It reduces accountability (can be good or bad)
- Can reduce bias (opinions) based on the speaker

Anonymity

But only the data being anonymous is not enough.

With enough **metadata** and combining different data sets, diversity can be eliminated

So, what to do?

… I’m not sure. But we can try:

- Always ask for consent
- Always use opt-in
- Evaluate the balance between use benefit and privacy
- Verify the regulations in your industry
- And always ask: WCGW?

References

https://falkvinge.net/2012/07/19/debunking-the-dangerous-nothing-to-hide-nothing-to-fear/

https://jacquesmattheij.com/if-you-have-nothing-to-hide

https://www.eff.org/deeplinks/2013/11/busting-eight-common-excuses-nsa-surveillance

https://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/