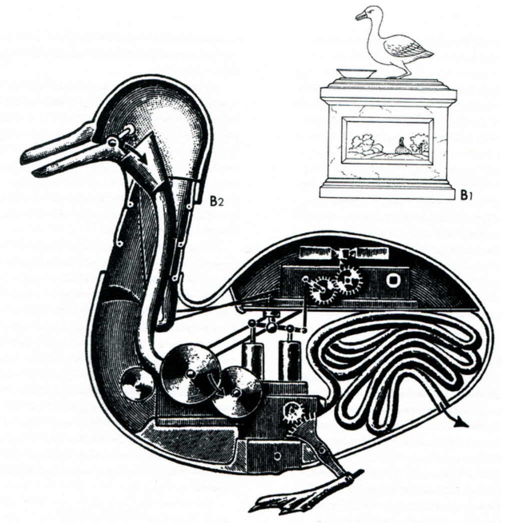
Can Authoritative Governments Abuse the Right to Access?

Cédric Lauradoux

June 24, 2022

A long time ago. . .

- **2017:** Duck Attack on Accountable Distributed Systems (Mobiquitous)
- **1739:** Vaucanson's digesting duck.



- If it poops like a duck, then it is a duck.
  Vaucanson's digesting duck poops like a duck. . .
  but it is not a duck!

Sometime ago. . .

- **2018:** I ask a company my data.
- **DPO says:** can you first provide a copy of your ID? I say no and I was very depressed.
- **DPO's thinking:** if the request includes the copy of Cedric Lauradoux's ID, then it is Cedric Lauradoux.
- **2019:** Security Analysis of Subject Access Request Procedures - How to Authenticate Data Subjects Safely When They Request for Their Data. (APF)

Did anything change?

- **Expectation:** nobody requests the copy of an ID to authenticate subject access requests.
- **Reality:** many DPOs still ask the copy of an ID to authenticate subject access requests.
  It makes me delusional. . .
- **Possible explanations:**
  - I am not convincing
  - Nobody cares

Really, nobody cares?

Authentication method	Attacks	Target
Copy of an ID	Social engineering [1] Falsification [2]	DPO DPO
Email confirmation	Email spoofing [2,3]	DPO
Bills	Falsification [1]	DPO
Personal question	Social engineering [1]	DPO

- [1] Pavur, GDPArrrrr: Using Privacy Laws to Steal Identities, Blackhat USA 2019.
- [2] Martino et al.: Personal Information Leakage by Abusing the GDPR 'Right of Access', SOUPS 2019.
- [3] Cagnazzo et al.: GDPiRated - Stealing Personal Information On- and Offline, ESORICS 2019.

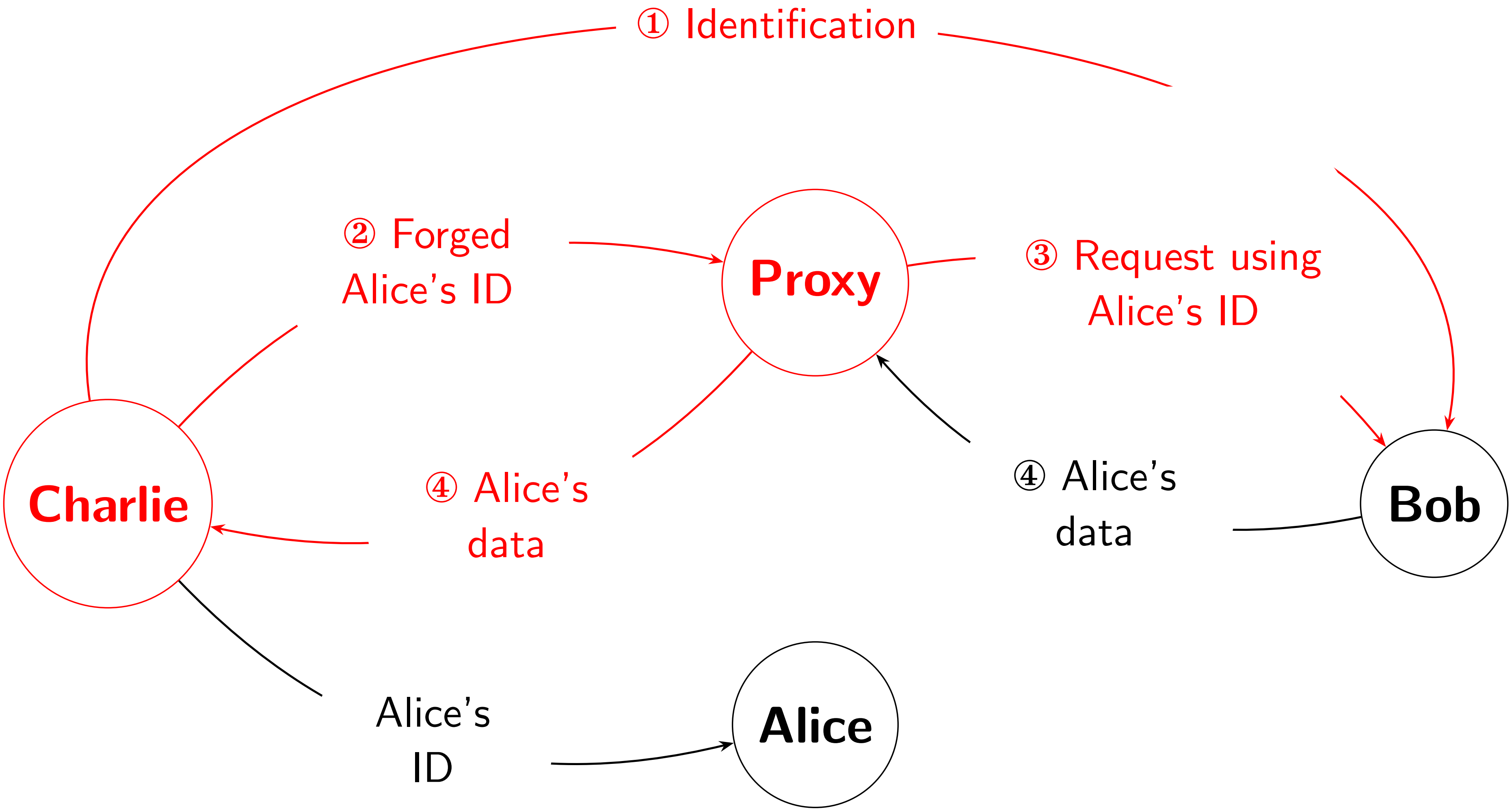
Maybe, I was not convincing!

- This is why I am here today!
  Let me tell you a GDPR's story.
- Bob manages a social network in Europe.
  (=data controller who has to respect the GDPR)
- Alice is a Dictatoria's native but she is a dissident.
  She protests using Bob's social network.
  (=data subject protected by the GDPR)
- Charlie is the undisputed ruler of Dictatoria.
  He is authoritative. Some call him a dictator. . .

One day. . .

- Bob receives an email which is a subject access request from Alice.
- Bob asks Alice to provide a copy of an ID.
  Bob receives the copy of Alice's ID.
- Bob thinks it is Alice who has submitted the request.
  Bob provides all the data he has related to Alice.
- **Later, Alice disappears.**
  This is a scary GDPR's story!

Charlie’s forgery attack



You need another story!

- Eve is a European's native, she is working at European Commission. She likes Bob's social network. (=data subject protected by the GDPR)

- One day, Eve visits Dictatoria for holidays.

- Later, Bob receives an email which is a subject access request. . .

- Eve was arrested for providing sensitive documents to Mister X. Eve was blackmailed by Mister X.

  I promise to never write fairy tales for kids!

What has really happened?

- When Eve has crossed Dictoria's borders, she had to show our passport.
- Borders officer has kept a high resolution picture of Eve's passport.
- This picture was later used to contact Bob to obtain all the data from Eve. It results that Charlie blackmails Eve.

First Conclusions

- **Why would a state abuse the right to access?**
  - Free/deniable/discret/automatable surveillance.
  - It looks too good to be true, but it is!

- This is why we need to fix the right to access.
  What are the options?
  - train DPOs
  - use stronger authentication methods!

Stronger authentication procedures?

- **Possible patches:**
  - ▷ deploy digital identity, (IPEN Webinar)
  - ▷ remote identity proofing, (ENISA's reports)
  - ▷ multiple-factors authentication. (Google Take Out)

- **Are these solutions compatible with the GDPR?**
  Recital 64 of the GDPR states that *A controller should not retain personal data for the sole purpose of being able to react to potential requests.*

Conclusion

- I hope that you are convinced that there are issues with how subject access requests are authenticated.
- It is critical to implement the right to access seriously.
- **More issues on the right to access:**

  Responses to EDPB's Guidelines 01/2022 on data subject rights - Right of access with **C. Santos**