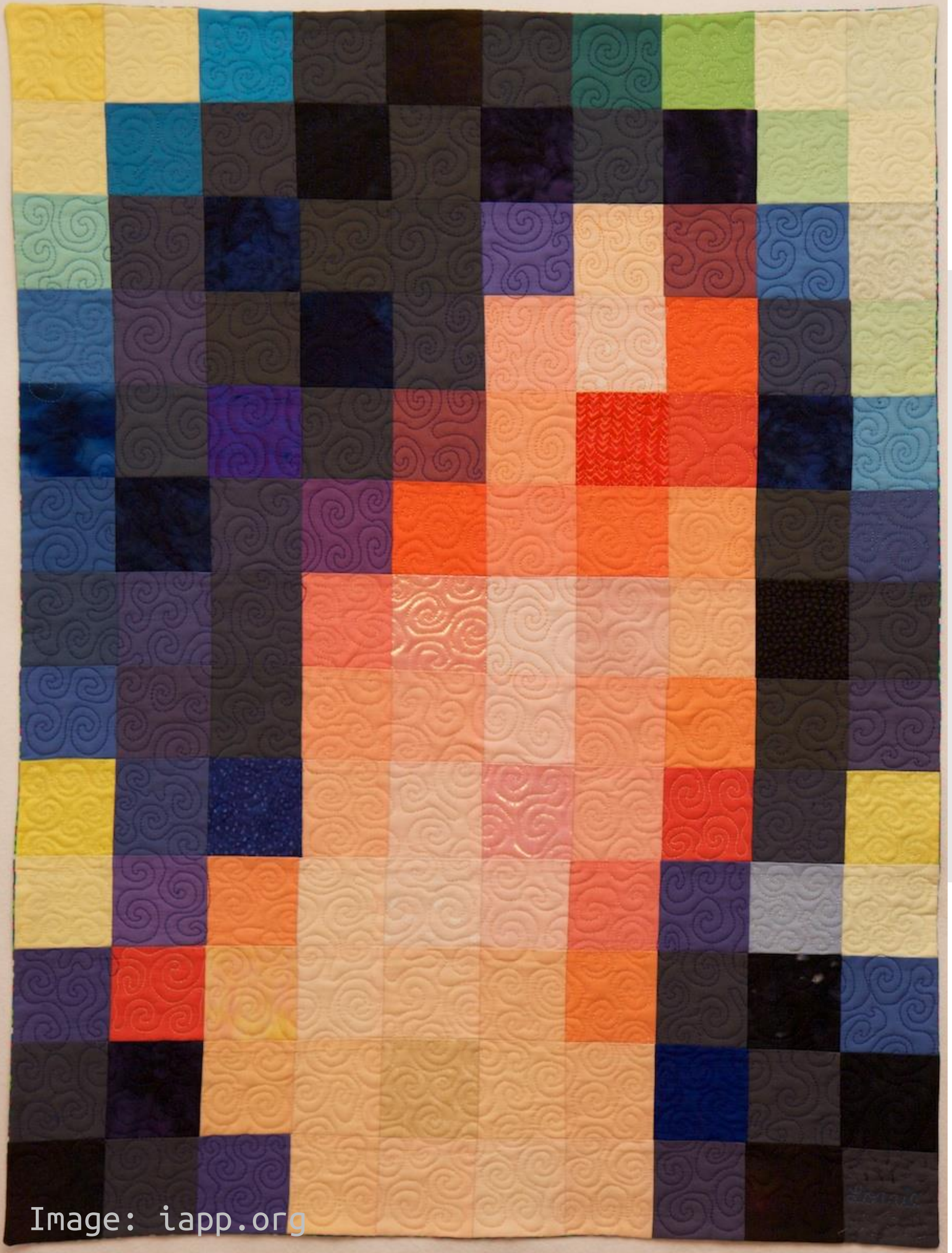


TPM ResilienceLab HEROS

Do we really need to violate people's privacy to build better models?

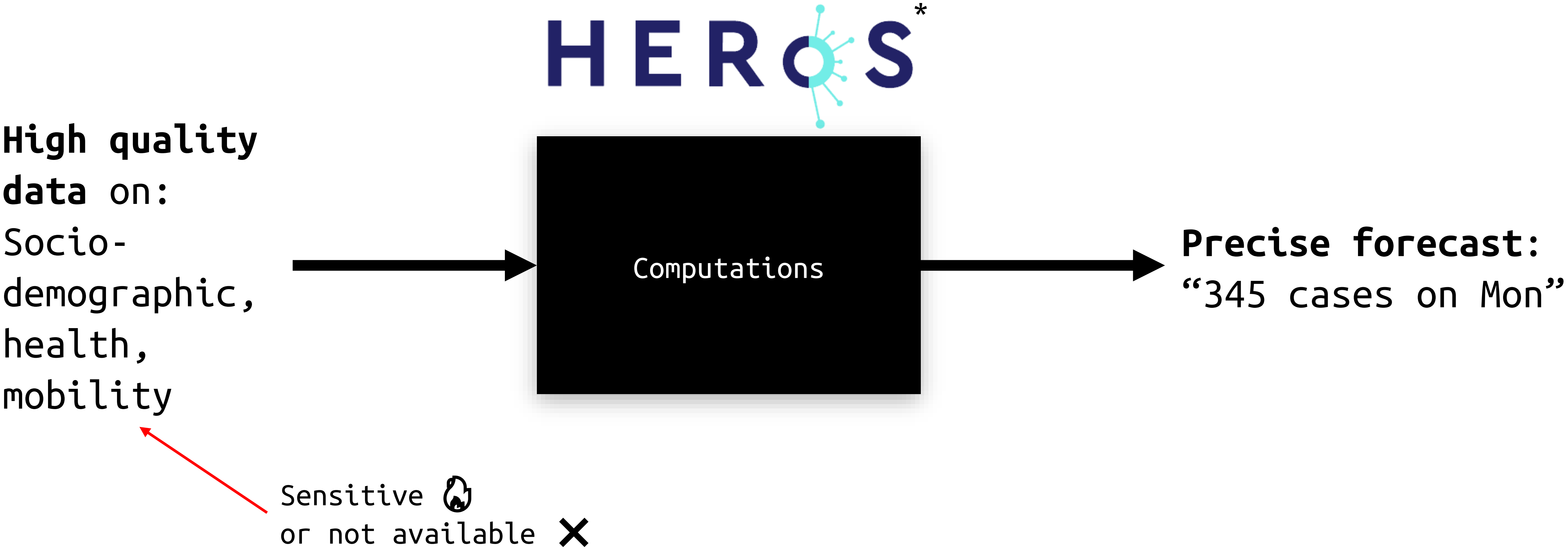
@mikhailsirenko

m.sirenko@tudelft.nl

What is a computer model?

You’re going to have a lunch soon!

Does the quality of the input matter?



HEROS*

High quality data on: Socio-demographic, health, mobility

Computations

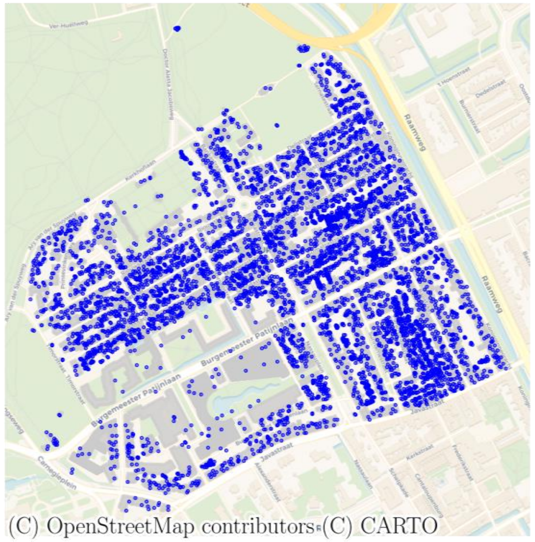
Precise forecast: “345 cases on Mon”

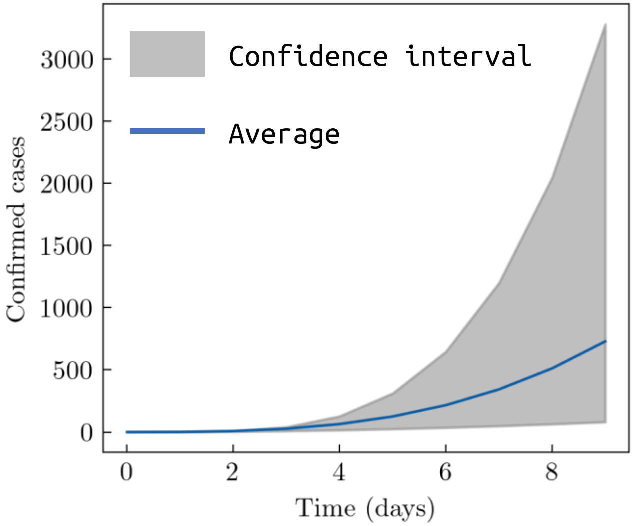
Sensitive 🔥
or not available ✕

* Read more about the model at https://heros-project.eu/output

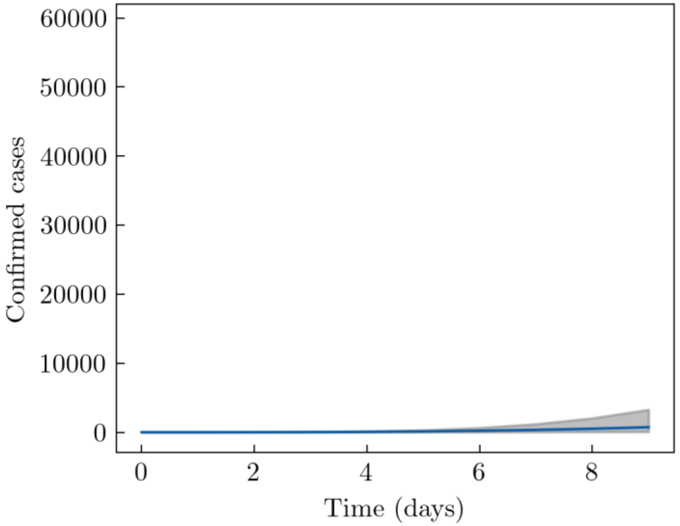
Do we really need to violate people’s privacy to build **precise** models?

High quality microdata:
Exact locations where
people live, sensitive 🔥

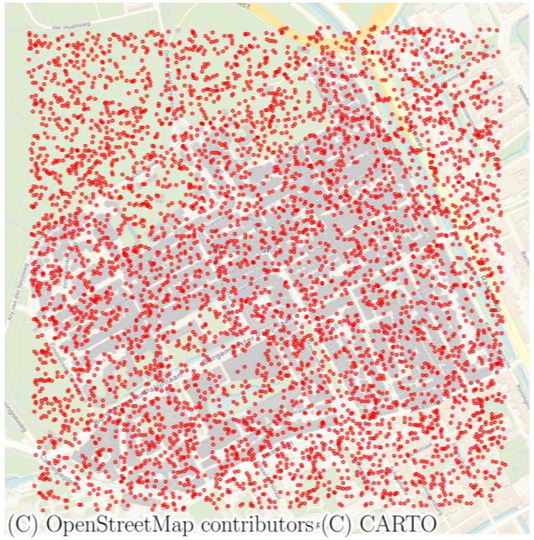


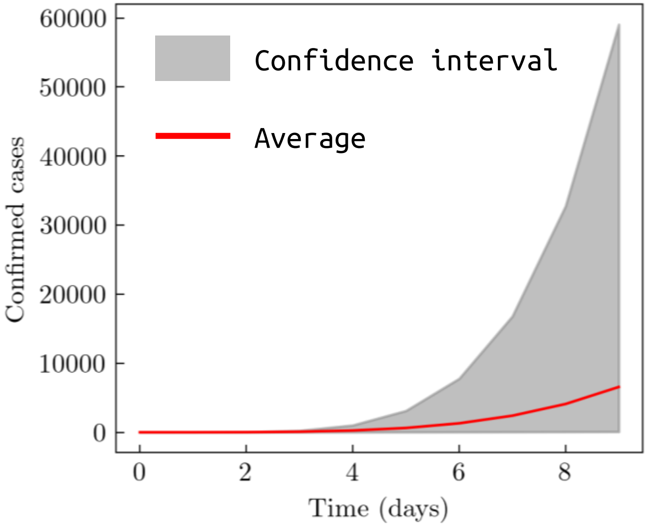


If y axis is shared

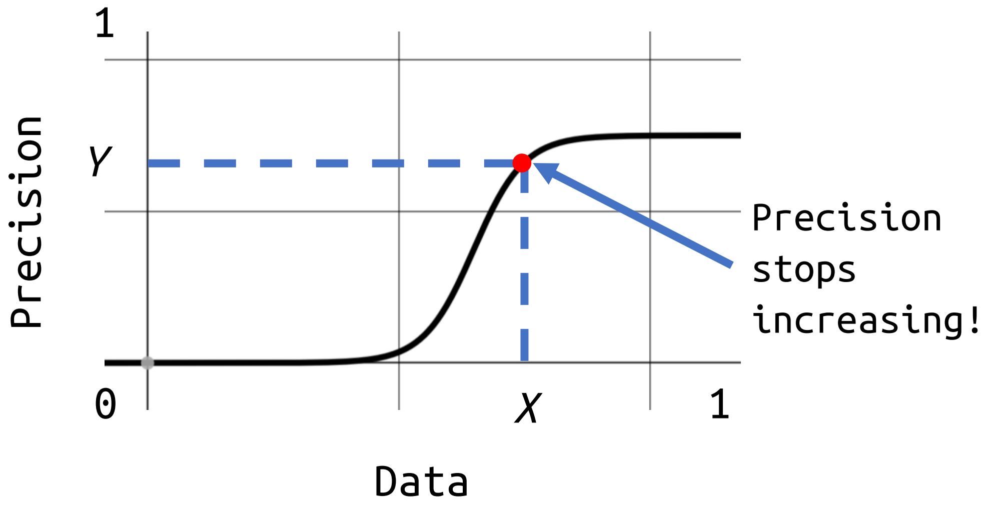


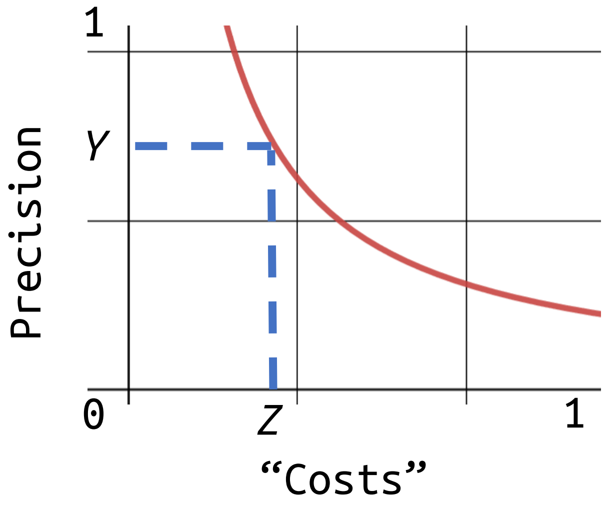
Open data:
Only a neighborhood where people
live, privacy preserved 🛡





Find the tipping point





Precision=1 extreme precision, a “crystal ball” 🔮
Precision=0.75 small confidence intervals
Precision=0.25 wide confidence intervals
Precision=0 it is better to toss a coin

Costs=1 extremely expensive, a “doomsday scenario” 💥
Costs=0.75 high expenses
Costs=0.25 low expenses
Costs=0 no expenses

X data will give us *Y* precision
but at the price of privacy

Y precision will help us to achieve
Z “costs”, **but again, at the price of privacy**

At some point, **microdata does not increase the precision of the model**. To preserve privacy and given that the **future is uncertain**, we must focus on using **open data** and designing **robust policies*** that account for numerous plausible scenarios.

* A robust policy is a policy that will work no matter what, e.g. virus parameters, will occur.

Meet the team