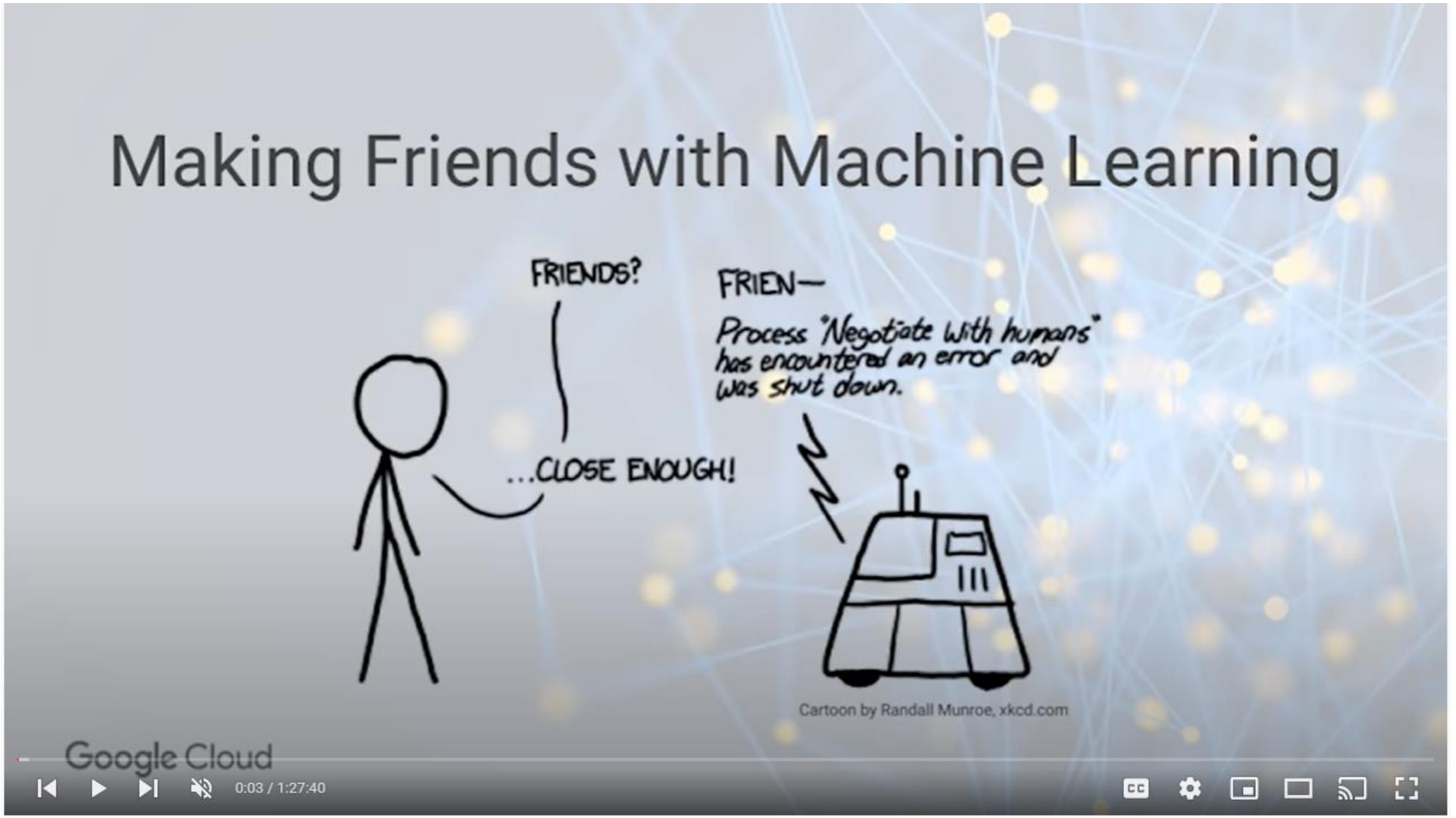
Best Practice Analytics

Part 1 – The Big Picture

Dr Detlef Nauck
Head of AI & Data Science Research

Please watch this 6 hour course by Cassie Kozyrkov

Introduction to ML and AI - MFML Part 1 - YouTube



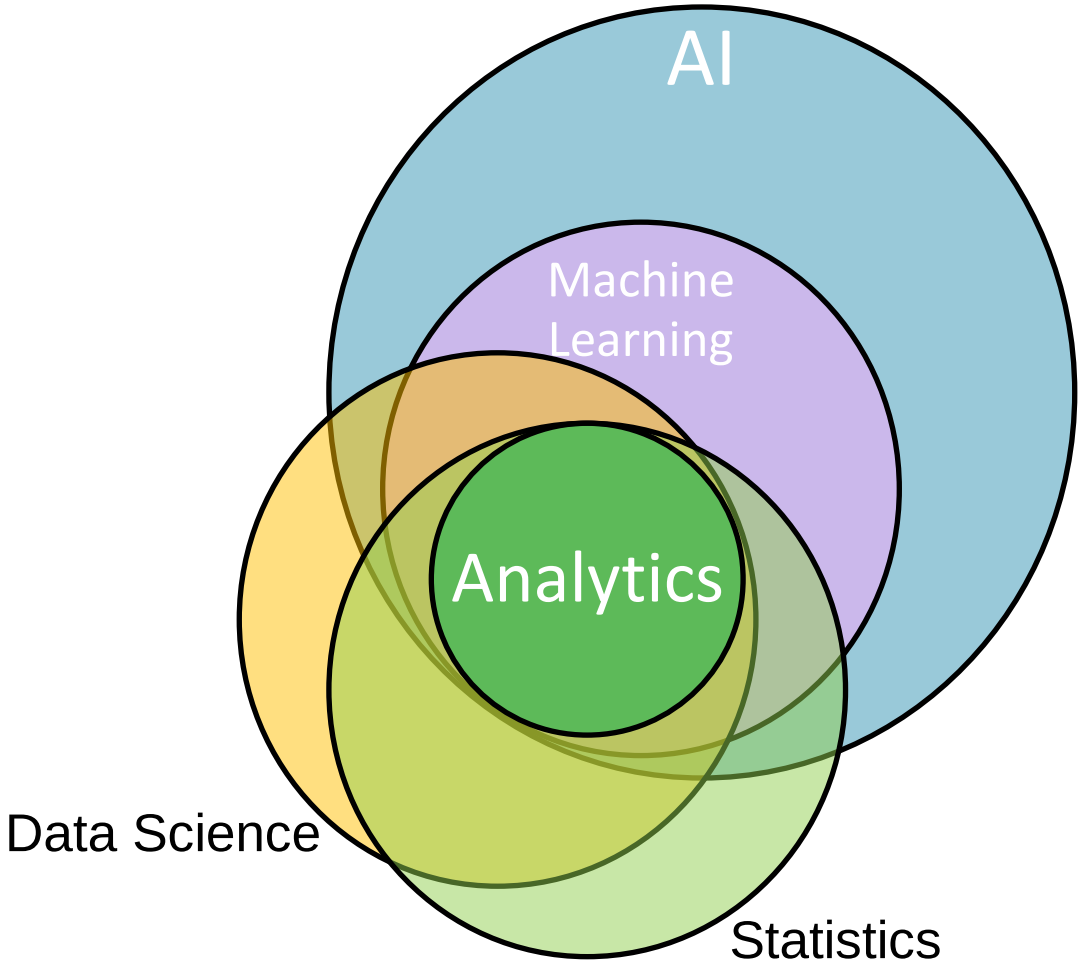
I suggest following Cassie Kozyrkov, Chief Decision Scientist at Google

@QUEASITA on Twitter
https://twitter.com/quaesita

Medium Blog:
https://kozyrkov.medium.com/

YouTube Channel:
https://www.youtube.com/c/Kozyrkov

Defining Some Words



Analytics: The scientific process of turning data into insight for making better decisions (INFORMS).

Statistics: The mathematical body of science that pertains to the collection, analysis, interpretation or explanation, and presentation of data (Wikipedia).

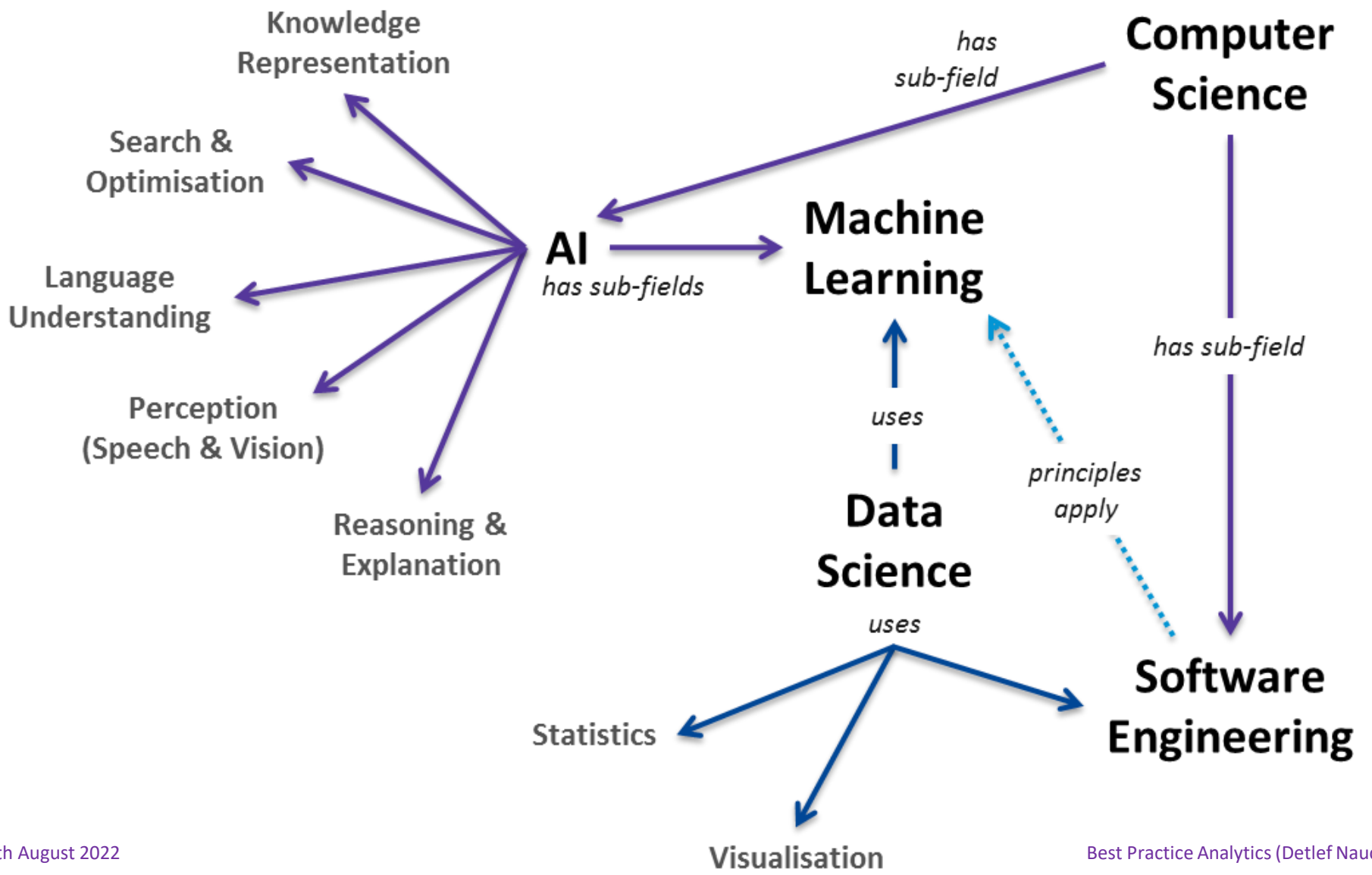
Data Science (DS): An interdisciplinary field that uses statistics and machine learning for (data) analytics with the aim of improving decision making through the extraction of knowledge and insights from data.

Machine Learning (ML): A field in Computer Science and AI that looks for algorithms that can automatically improve their performance at a task without explicit programming but by observing relevant data.

Artificial Intelligence (AI): the study of "intelligent agents": any system that perceives its environment and takes actions that maximize its chance of achieving its goals (Wikipedia, AI Textbooks).

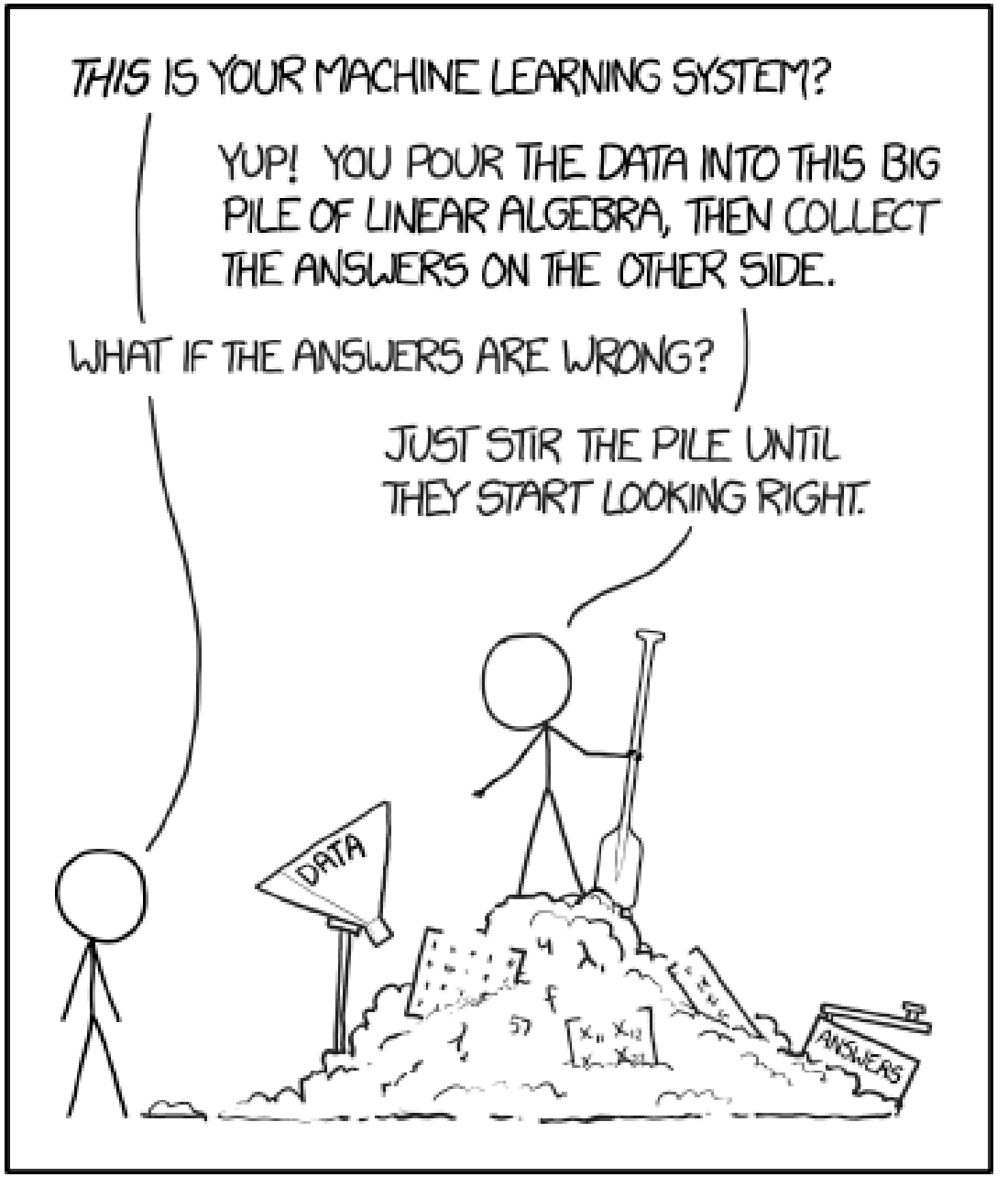
Or, more pragmatically: Artificial Intelligence is the ability of a machine to display intelligent behaviour. By “intelligent” we mean an activity that we would normally expect a human to perform (e.g. reasoning, speech, vision), which a machine performs by perceiving, analysing and adapting to data about its environment.

AI – ML – DS Taxonomy



Key Takeaways – Data Analytics and Machine Learning require

- Testing
- Governance
- Orchestration



https://xkcd.com/1838/

The Ethical Dimension of AI, ML and Data Science

- What should AI and Data Science be used / not used for and what is the impact on society such as privacy and automation of jobs?

- GDPR

- For example no black box models if decisions significantly affect a person. Organisations must be able to explain their algorithmic decision making in certain conditions.

- Bias – (unfair) under / over-representation of subgroups in your data

- Bias in data and models not only makes models perform worse, it can also damage a brand.

http://www.wsj.com/articles/wisconsin-supreme-court-to-rule-on-predictive-algorithms-used-in-sentencing-1465119008

https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software/

▲ We might be tempted to call them 'frankenalgos' - though Mary Shelley couldn't have made this up. Illustration: Marco Goran Romano

Franken-algorithms: the deadly consequences of unpredictable code

The death of a woman hit by a self-driving car highlights an unfolding technological crisis, as code piled on code creates 'a universe no one fully understands'

https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger

Challenges in Analytics (especially Machine Learning)

Data Provenance

Where does the data come from, how was it collected and can I trust it?

Data Quality

Is the data error free?

Data Bias

Does the data accurately reflect the population/situation I want to model? What is missing?

Model Bias

Driven by unconscious bias or data bias – does my model treat everybody fairly?

Model Comprehension

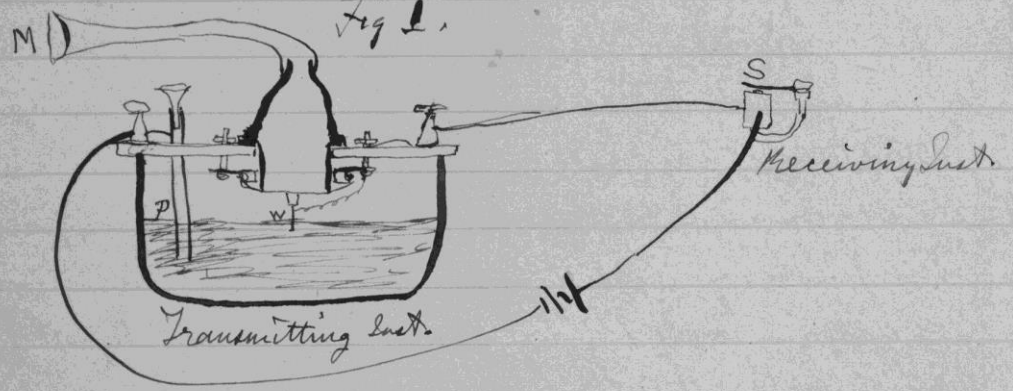
Why are the outputs of my (black box) models the way they are?

Ethics

Can I use this data? Do decisions made by models affect people? Is there discriminatory bias? …

March 10th 1876

Fig 1.



1. The improved instrument shown in Fig. I was constructed this morning and tried this evening. P is a brass pipe and W the platinum wire M the mouth piece — and S the armature of the Receiving Instrument.

W. Watson was stationed in one room with the Receiving Instrument. He pressed one ear closely against S and closed his other ear with his hand. The Transmitting Instrument was placed in another room and the doors of both rooms were closed.

I then shouted into M the following sentence: "Mr. Watson — Come here — I want to see you". To my delight he came and declared that he had heard and understood what I said.

I asked him to repeat the words — ~~He said~~ He answered "You said 'Mr. Watson — come here — I want to see you'." We then changed places and I listened at S while W. Watson read a few passages from a book into the mouth piece M. It was certainly the case that articulate sounds proceeded from S. The effect was loud but indistinct and muffled.

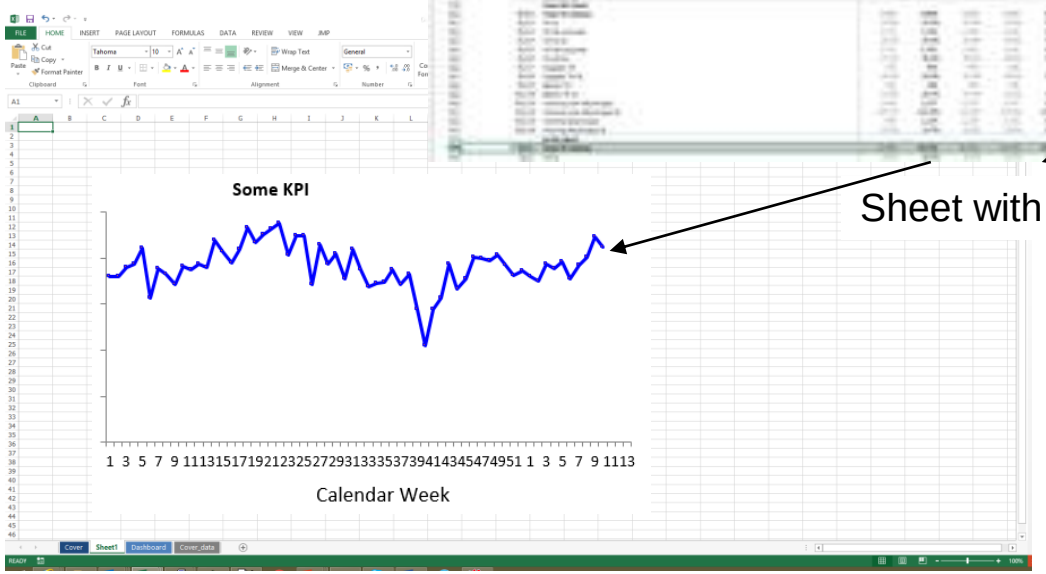
If I had read beforehand the passage given by Mr Watson I should have recognized every word. As it was I could not make out the sense — but an occasional word here and there was quite distinct. I made out "to" and "out" and "further"; and finally the sentence "Mr Bell Do you understand what I say? DO-YOU-UNDER-STAND-WHAT-I-SAY" came quite clearly and intelligibly. No sound was audible when the armature S was removed.

Why We Need Best Practice Analytics

A Typical Spreadsheet-based Reporting Scenario

Decision maker

Weekly report in a spreadsheet

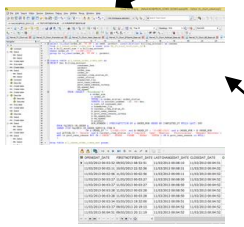


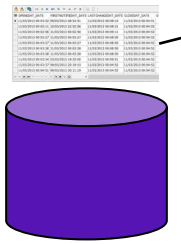
Cover sheet with selected charts

Sheet with hundreds of KPIs

Business owner of KPI receives a weekly number

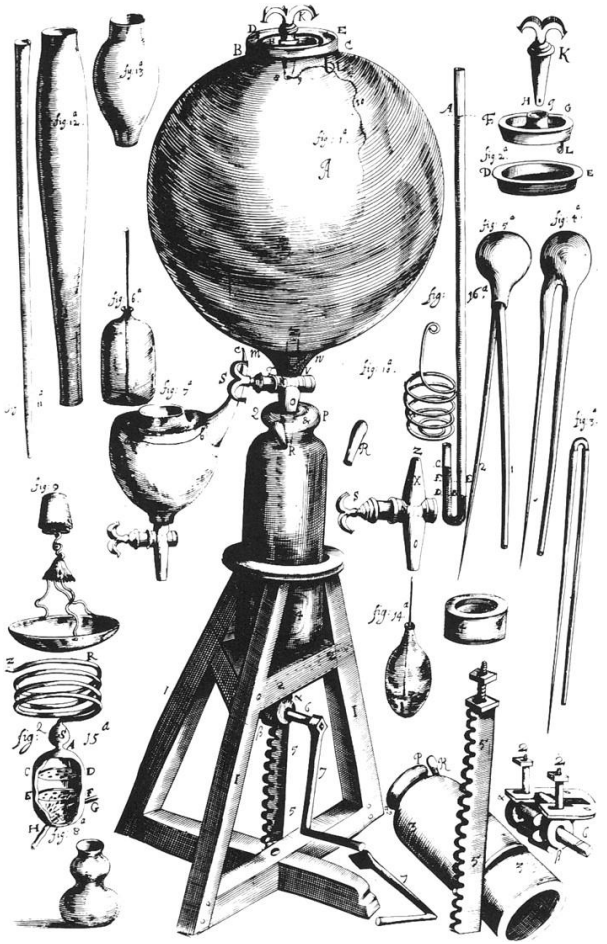
IT personnel using undocumented scripts to produce tables in personal schemas





Undocumented table in enterprise data warehouse

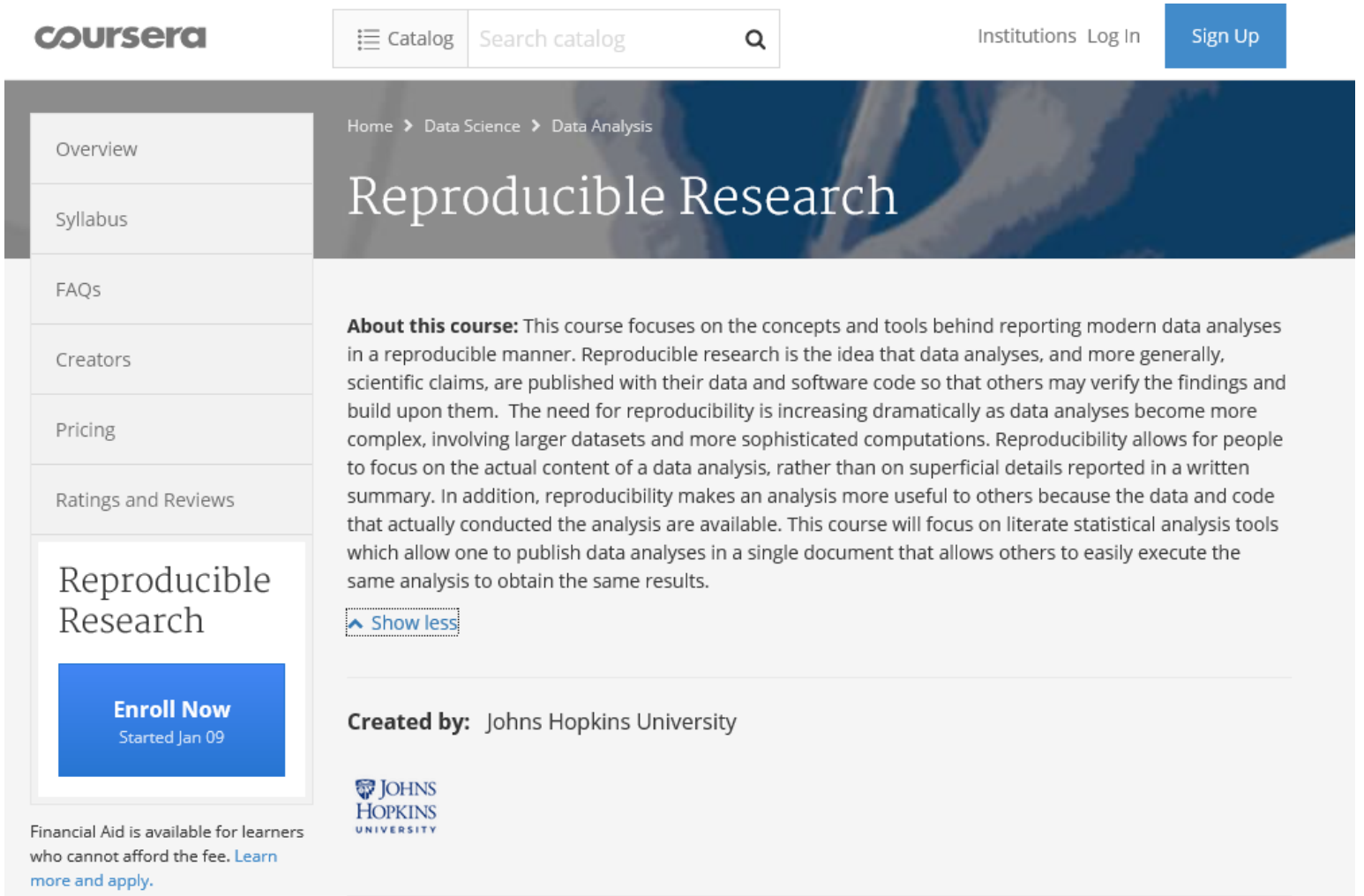
Reproducibility



Boyle's air pump (see https://en.wikipedia.org/wiki/Reproducibility)

- Reproducibility is the ability of an entire experiment or study to be duplicated (by someone else).
- Reproducibility is one of the main principles of the scientific method.
- Reproducible does not mean correct
- Your analysis/claims can be reproducible and can still be wrong
- Reproducibility is the only thing an analyst can guarantee about a study.

Reproducible Research – Online Course



https://www.coursera.org/learn/reproducible-research

Best Practice Analytics – Reproducible Research

- Reproducible does not mean correct
- Your analysis/claims can be reproducible and can still be wrong
- Reproducibility is the only thing an analyst can guarantee about a study.
- Example: Thomas Piketty's book on 'Capital in the Twenty-First Century'.
  All the data and analysis has been made available on the web
  http://piketty.pse.ens.fr/en/capital21c2


FINANCIAL TIMES
ft.com/globaleconomy

Home UK World Companies Markets Global Economy Lex Comment
Economic Calendar Africa Americas Asia China EU India Middle East UK US

May 23, 2014 7:00 pm

Piketty findings undercut by errors

By Chris Giles in London

Share Author alerts Print Clip Comments

Economist and author Thomas Piketty

Thomas Piketty's book, 'Capital in the Twenty-First Century', has been the publishing sensation of the year. Its thesis of rising inequality tapped into the

Big Data is transforming the economics of data processing

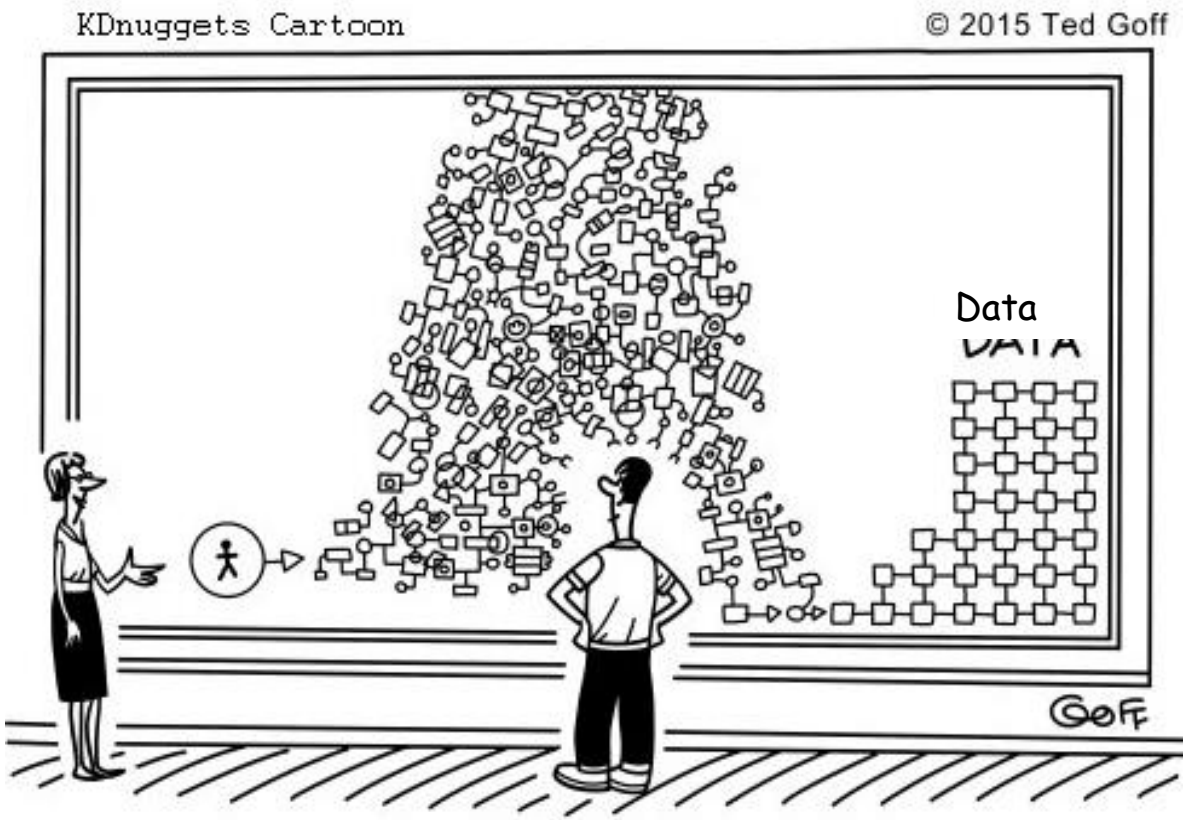
In **1980** storing and querying a year's worth of 147TB twitter data (if it existed) would have required a spend of **75%** of the **Apollo program** ($38.4bn in inflation adjusted 1980 US Dollars).

In **2014** it cost approximately the same as a small used car (**£6k**).

In **2021** a 150TB storage array (HP ProLiant SL4540 Gen 8 Storage Server, 50x3TB SAS) costs **£4k**.

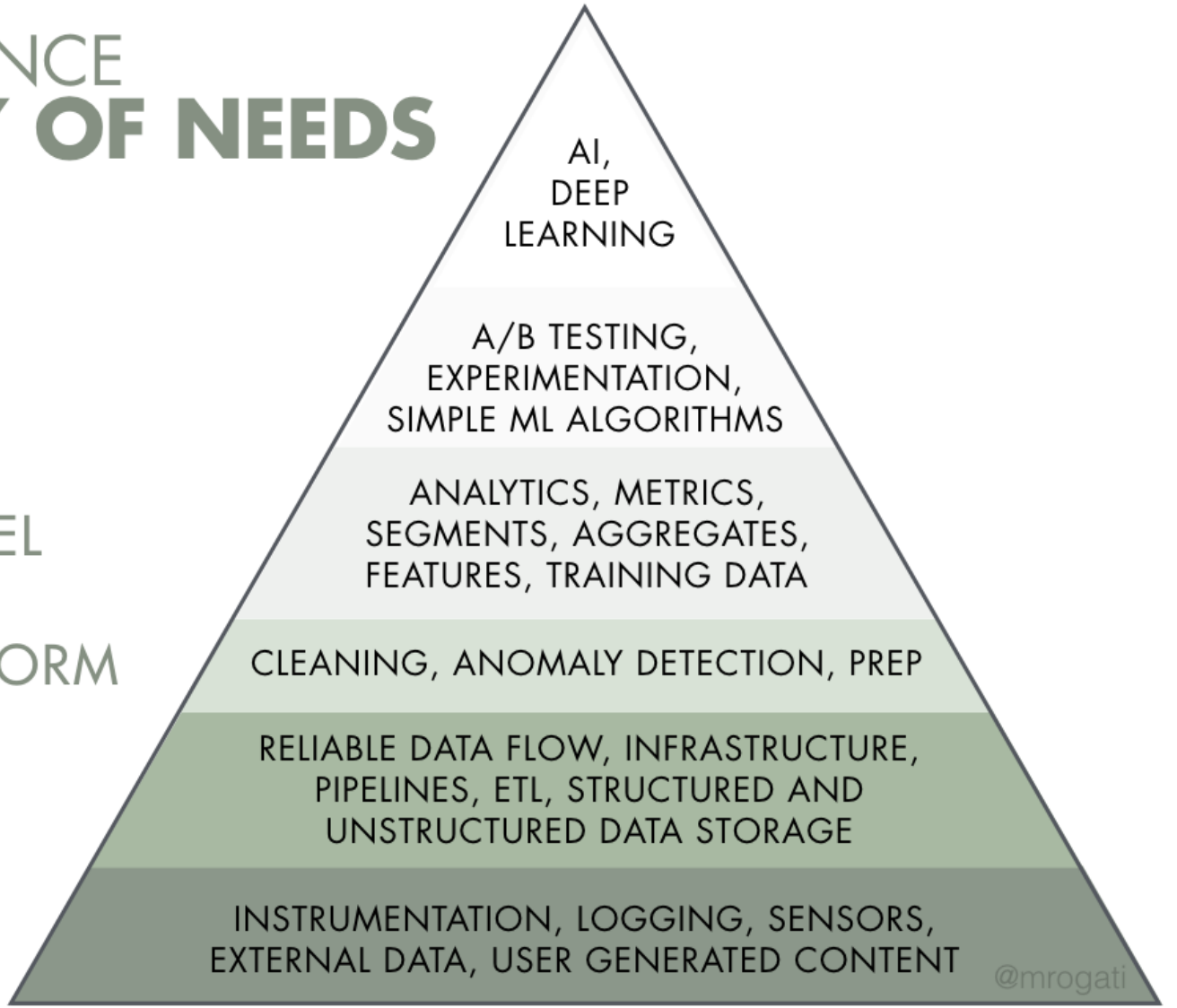
Data Quality Issues in Enterprises

- Operational data schemas are not designed for analytics.
- Data is distributed across silos and access can be difficult
  (administrative and computational obstacles).
- Data inconsistencies make joining data across operational domains difficult and error prone.
- It won't get better (human nature, operational pressure, lack of business case). Actually, Big Data makes it worse.
- Effort in data preparation is and will remain typically 80%-90% of project effort.



"This is you, these are organisational and regulatory obstacles, and this is the operational data you want. Welcome to the Data Science Team!"
(Original at http://www.kdnuggets.com/2015/03/cartoon-us-chief-data-scientist-challenge.html)

THE DATA SCIENCE HIERARCHY OF NEEDS



Monica Rogati: The AI Pyramid of Needs. Hacker-noon blog post, 1 Aug 2017 (https://hacker-noon.com/the-ai-hierarchy-of-needs-18f111fcc007, accessed 19/04/2018).

Perception Problem about Machine Learning

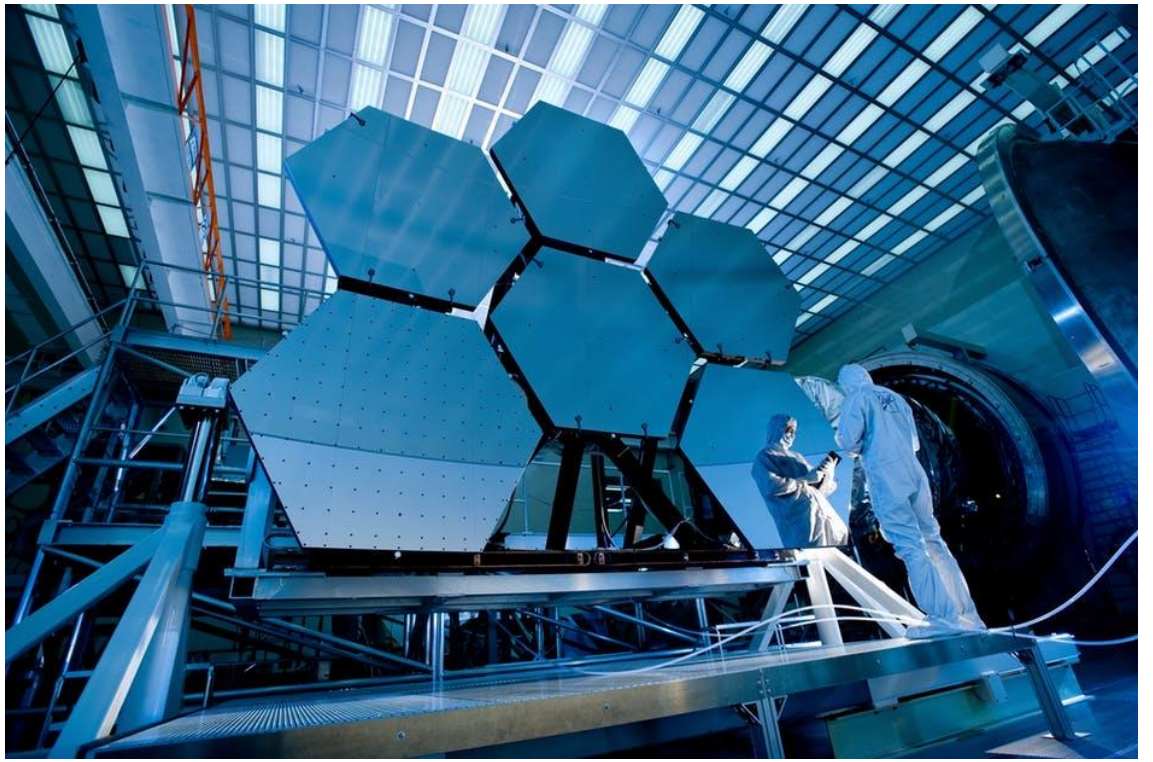
The AI & Machine Learning Office

This is where you would like to work

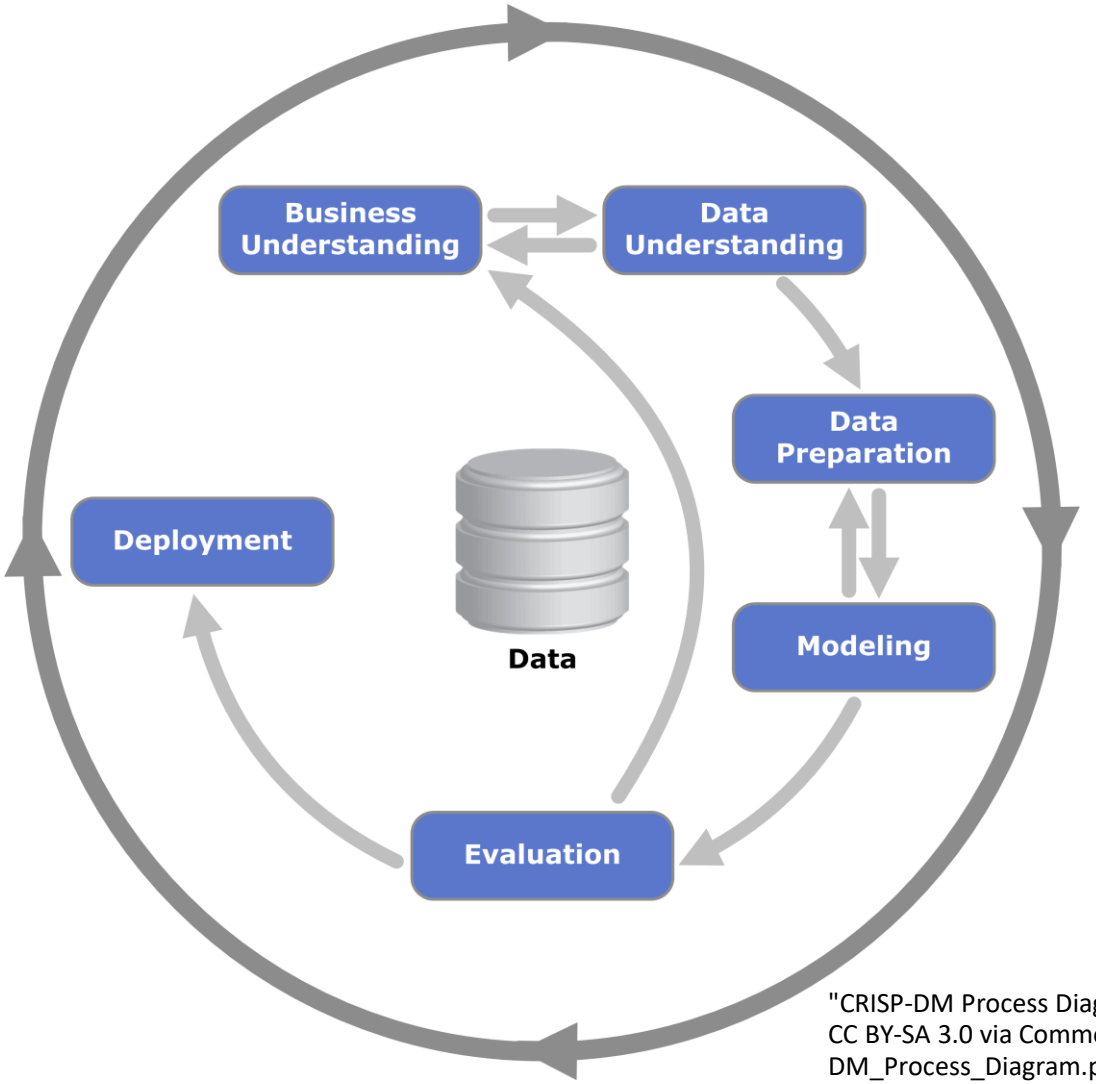
The Data Mine

This is where you will spent most of your time

Data Science: From Cottage Industry to Engineering and Automation



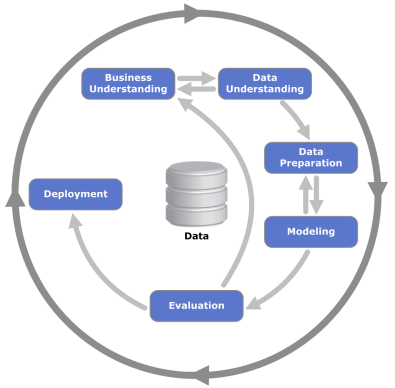
The Process of Data Science



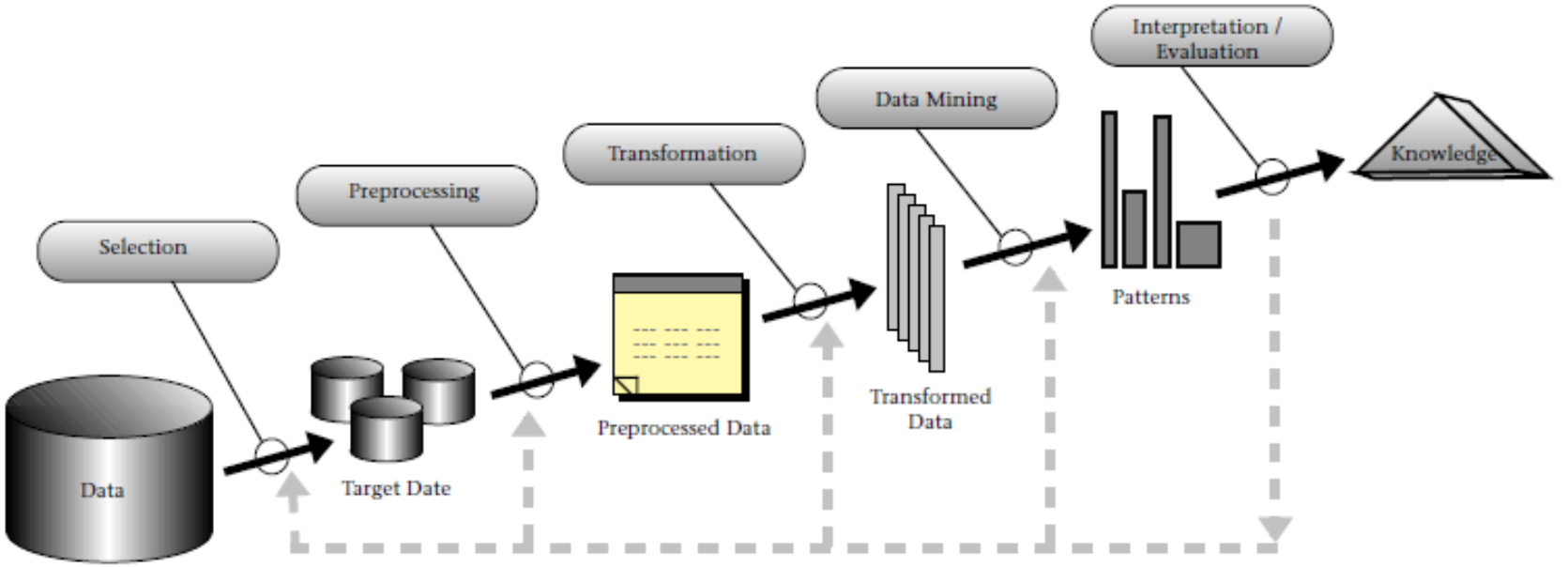
Cross Industry Standard Process for Data Mining

"CRISP-DM Process Diagram" by Kenneth Jensen - Own work. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:CRISP-DM_Process_Diagram.png#/media/File:CRISP-DM_Process_Diagram.png

The Process of Data Science

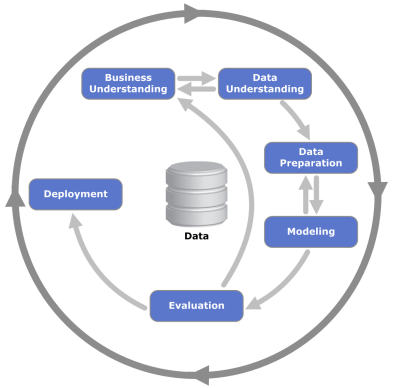


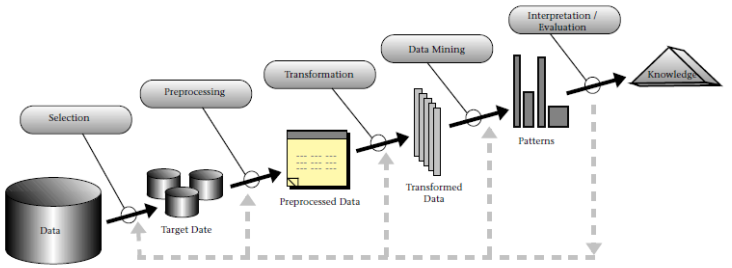
Steps that compose the KDD Process



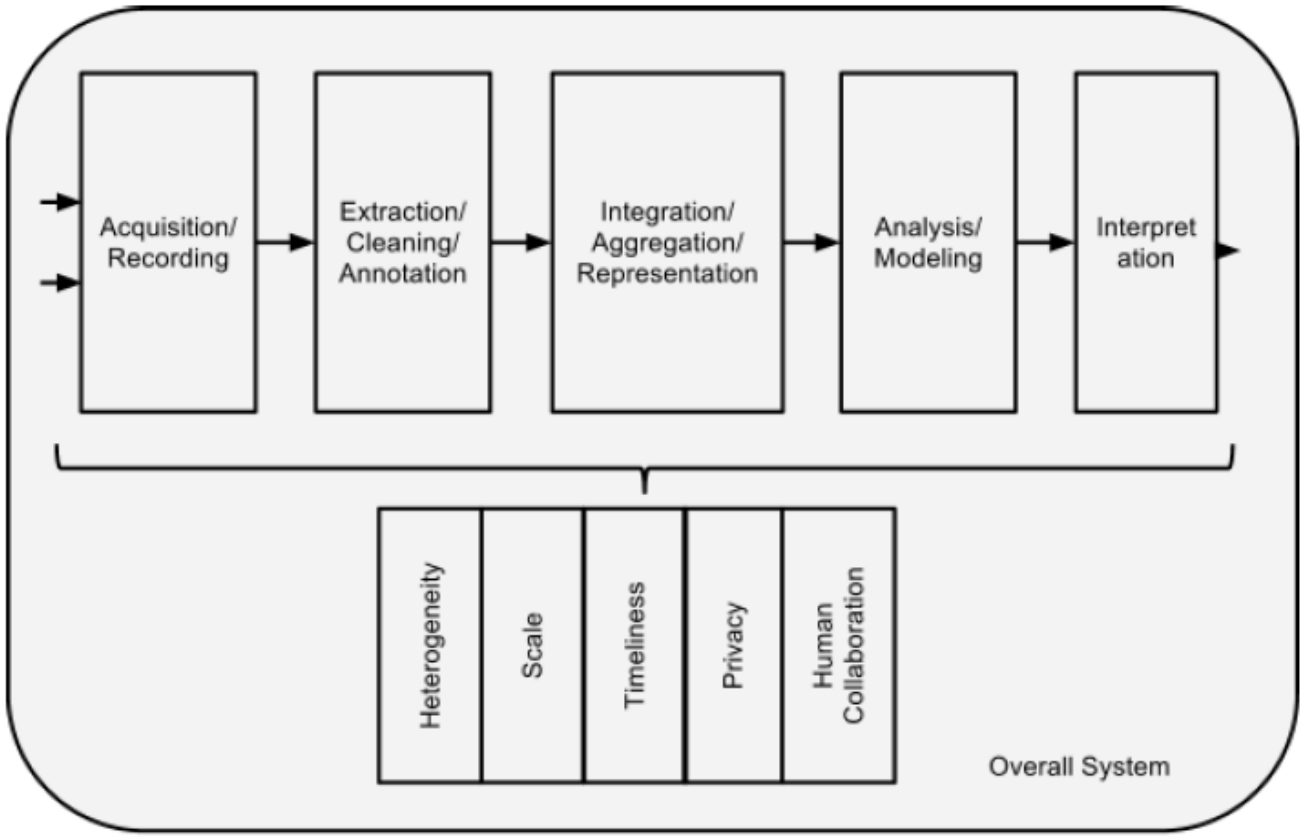
U. Fayyad, G. P.-Shapiro, and P. Smyth. From data mining to knowledge discovery in databases. AI Magazine, 17(3):37-54, Fall 1996

The Process of Data Science



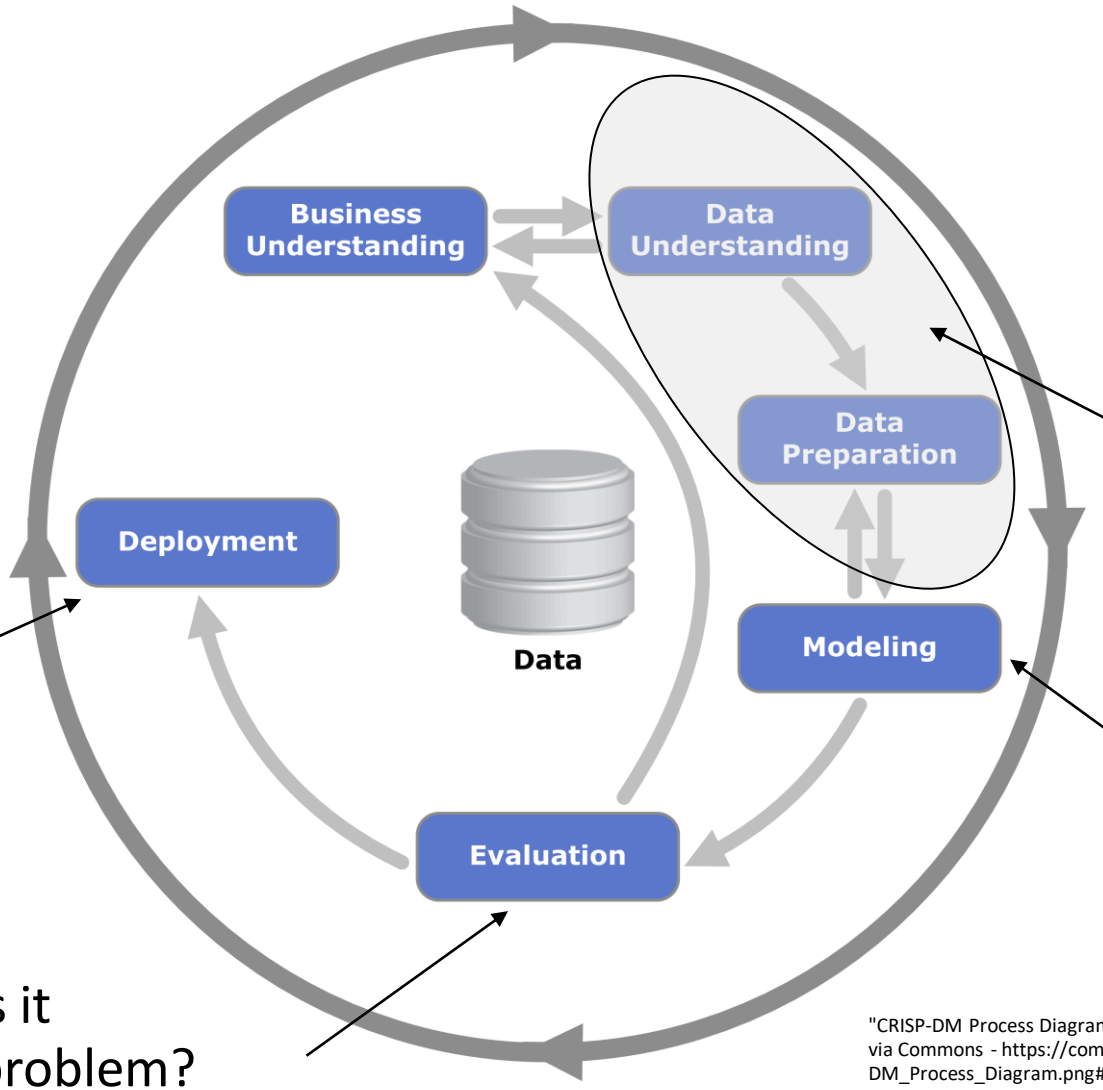


Big Data Analysis Pipeline



Challenges and Opportunities with Big Data. Computing Community Consortium Big Data Whitepaper: http://cra.org/ccc/wp-content/uploads/sites/2/2015/05/bigdatawhitepaper.pdf.

The Process of Data Science – Let's use this one



Cross Industry Standard Process for Data Mining

Data Wrangling:
includes data access, exploratory data analysis and data transformation.
70%-90% of project effort

Analytics:
Building and testing models

95% of failed projects fail at deployment
[myth or reference?]

Reality check – does it solve the business problem?

How to Run a Data Analysis Project

Governance has similarities with software development projects

Requirements
- Define the scope of the analysis
- Identify data sources

Provenance
- Where does the data come from, what is the data quality?
- What analysis methods and tools have been used?

Documentation
- What has been done to the data (pre-processing, variable selection, …)?
- How has the analysis been carried out, what models have been produced, what parameters have been selected, what were the unsuccessful attempts? …
- What does the analysis outcome mean?

Test
- What tests have been carried out to validate the analysis results?

Reproducibility
- Is there versioning of data and analysis methods available?
- For how long will the data and the analysis software be available? Where is all of it?

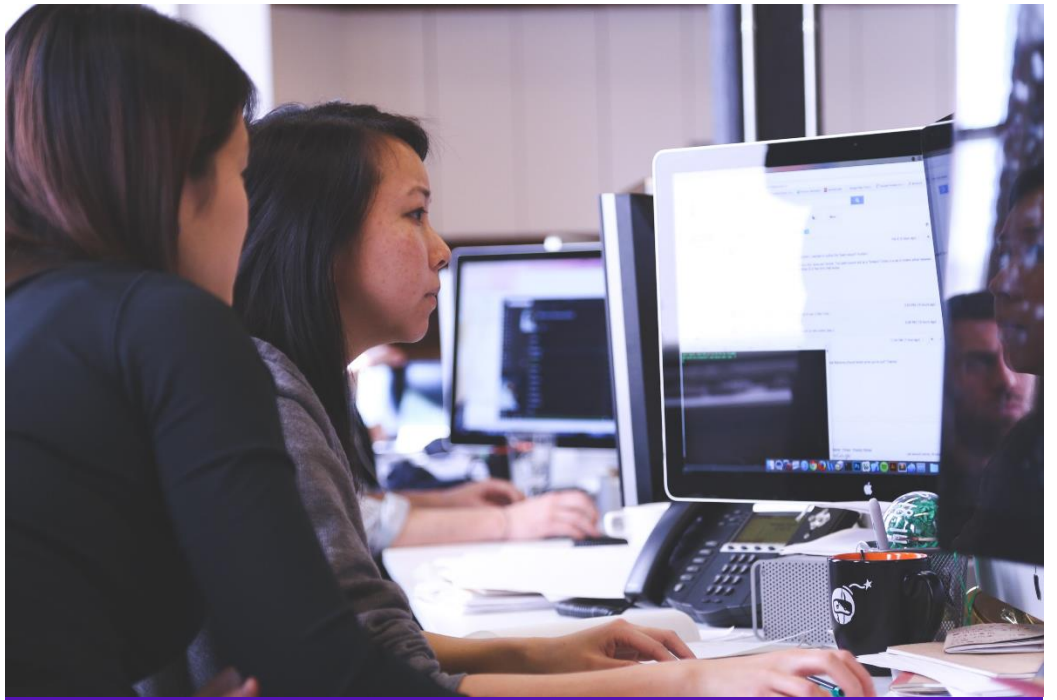
Policies and Risk Management
- Who can access data and models?

Problem: There is no agreed governance standard.
(Compare software quality standard ISO/IEC 9126
https://en.wikipedia.org/wiki/ISO/IEC_9126)

Test Driven Analytics (TDA) – Learn from Software Development

How do you make sure that your analysis is correct?

- Is your data any good?
- Have you validated your model?
- Do decisions taken have the expected business impact?



Test-driven development (TDD) is an advanced technique of using automated unit tests to drive the design of software and force decoupling of dependencies. The result of using this practice is a comprehensive suite of unit tests that can be run at any time to provide feedback that the software is still working (Microsoft: Guidelines for test-driven development)

"Machine learning is an approach to making repeated decisions that involves algorithmically finding patterns in data and using these to make recipes (models) that deal correctly with brand new data."

(Cassie Kozyrkov: Making Friends with Machine Learning)

Be warned:

Machine Learning scales stupid!

Or

With automation you can
make more mistakes
in a shorter amount of time.

ML is the ultimate GIGO

The world represented by your data is the only world you can expect to succeed in.

There is no way this goes past my well-designed input parser

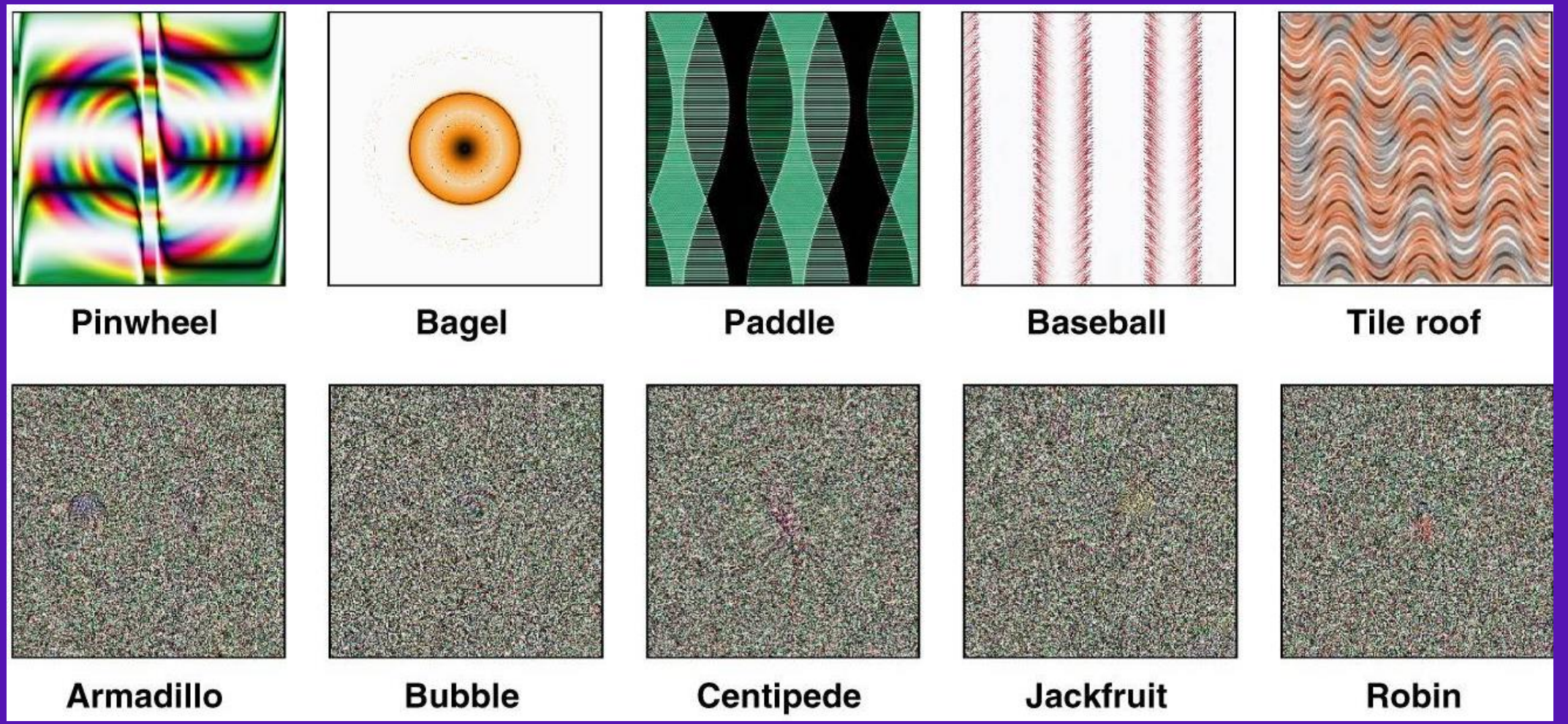
Source: https://muppet.fandom.com/wiki/Sam_the_Eagle

I'll take anything

Source: https://muppet.fandom.com/wiki/Oscar_the_Grouch

Software **Machine Learning**

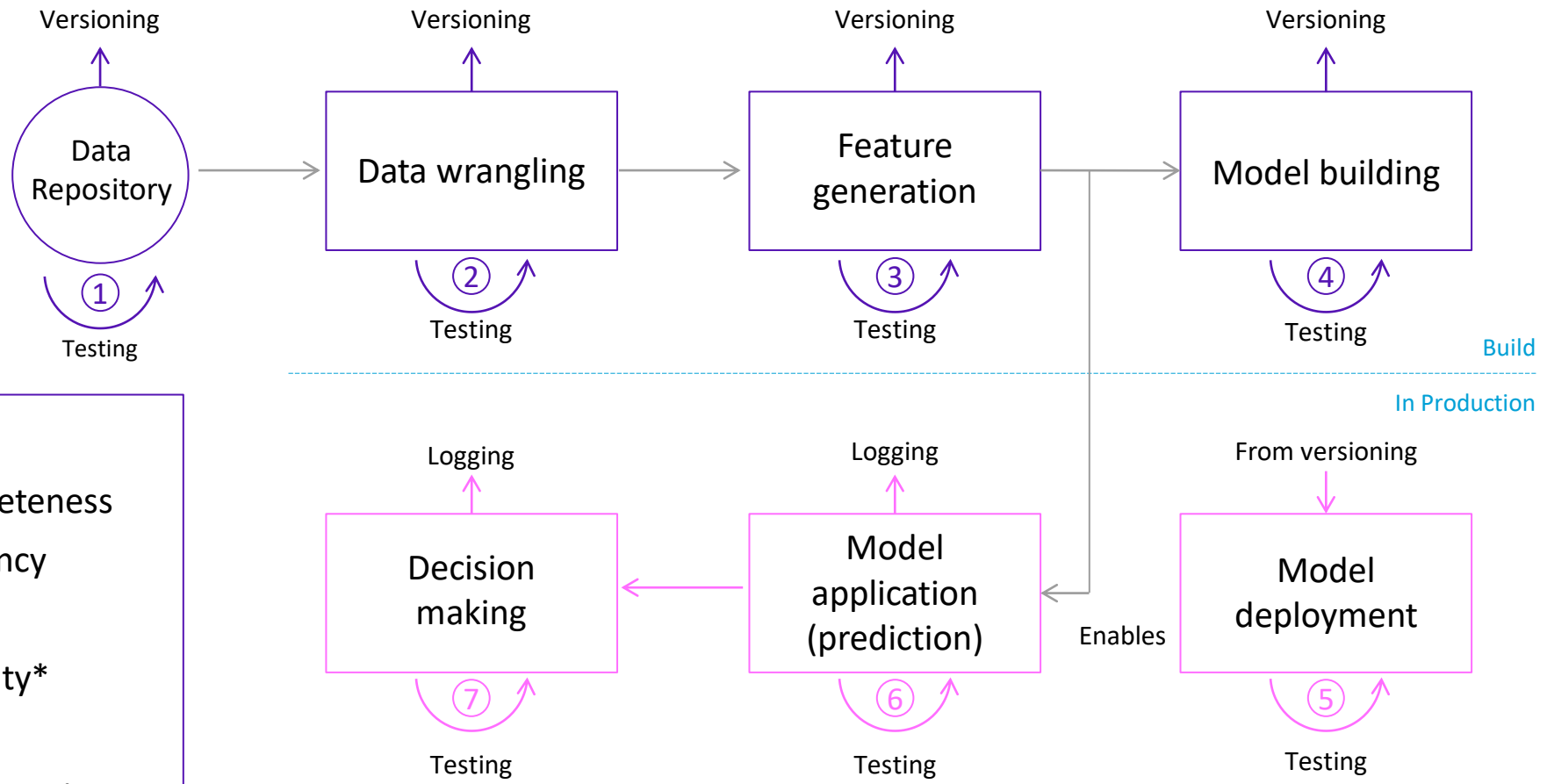
Garbage-in-Garbage-out: an AI model accepts anything as input and will produce an output



Zhenglong Zhou, Chaz Firestone: Humans can decipher adversarial images. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6430776/

Model Factories

Best Practice for AI, ML and Data Science Workflows with Integrated Continuous Testing



Test Scenarios

1. Data quality* and completeness
2. Data errors and consistency
3. Feature quality*
4. Code errors, model quality*
5. Model scalability
6. Model quality*, feature consistency
7. Control groups, business impact

*) quality = performance, fairness, usability, explainability …

Model Factories – Automation, Governance, Reproducibility

Not a single tool but a
highly automated production line.
Combining the tools that get the job done.

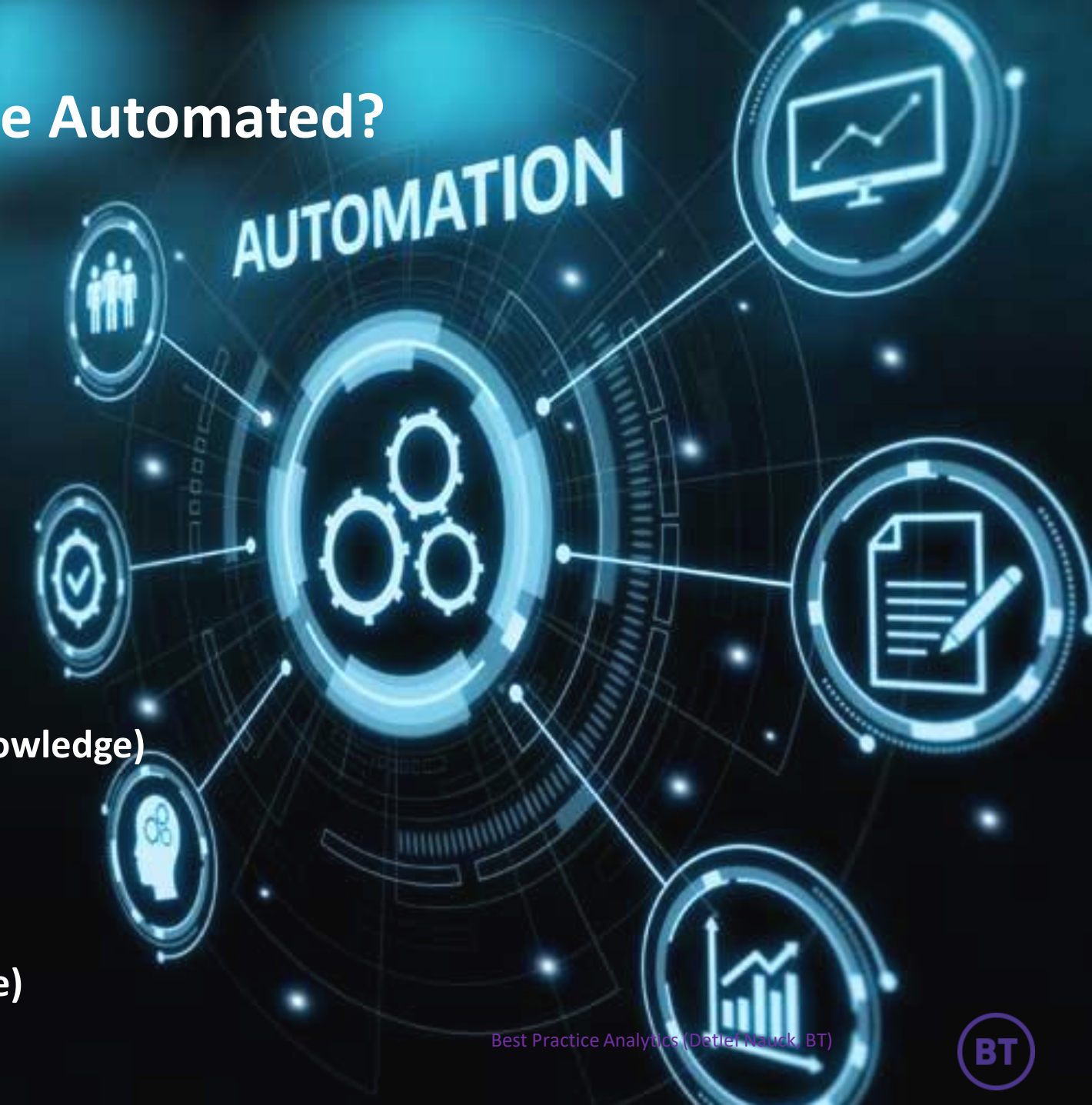
Potentially different tools in different cloud and on-premise environments.

Overlay of

- Versioning (e.g. Git, …)
- Testing (e.g. Selenium, …)
- Orchestration (e.g. Jenkins, …)
- Reporting (e.g. Shiny, Dash, …)
- Management (mlflow, Kubeflow, …)
- Governance (…)

Model Factories – What Can be Automated?

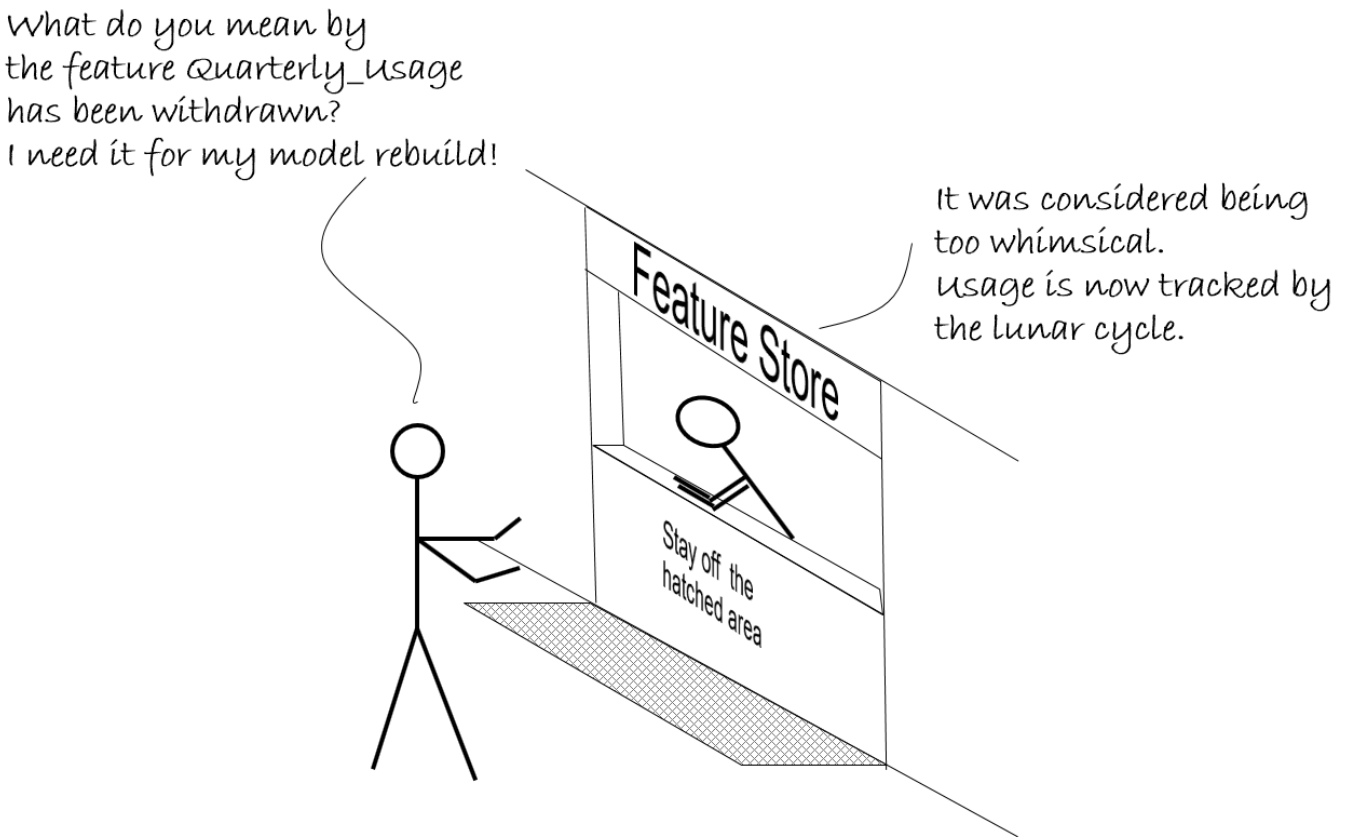
- **Relatively Straightforward (do!)**
  - Data pipelines
  - Model build and test
  - Deployment
  - In-life monitoring, i.e. decision test
  - Reporting
- **More Difficult (invest!)**
  - Data wrangling (needs tools)
  - Data quality monitoring (needs domain knowledge)
- **Hard (educate!)**
  - Feature crafting, bias/fairness evaluation (needs data science and domain knowledge)



Model Factory Components: Feature Store

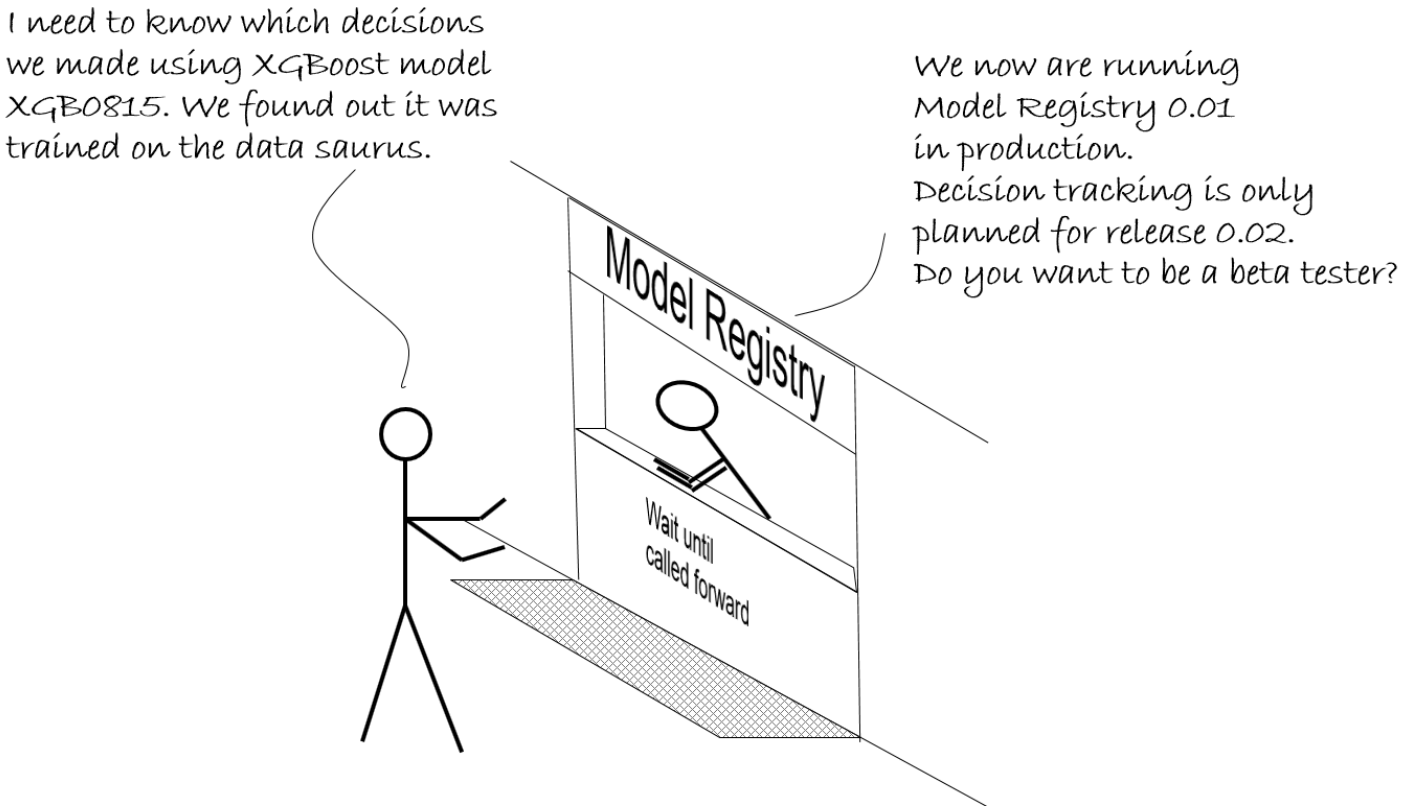
- Sharing features across models (accountability)
- Track feature quality (testing)
- Request feature values for a particular time
- Create, edit and branch features (versioning)
- Leverage community knowledge

Feature stores still have low maturity and limited capabilities, but cloud providers are working on them.



Model Factory Components: Model Registry

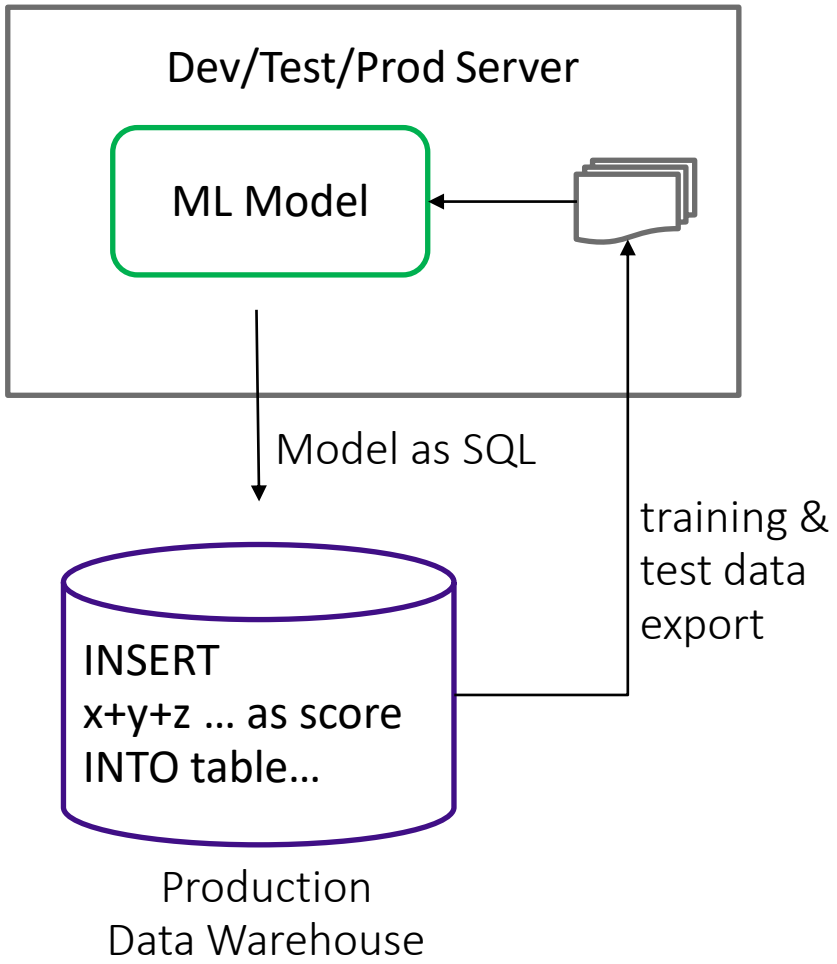
- Tracking models throughout their lifecycle
- Managing auto-deployment and model rebuild
- Run champion/challenger models
- Track decision making and business value
- Provides hooks into continuous testing

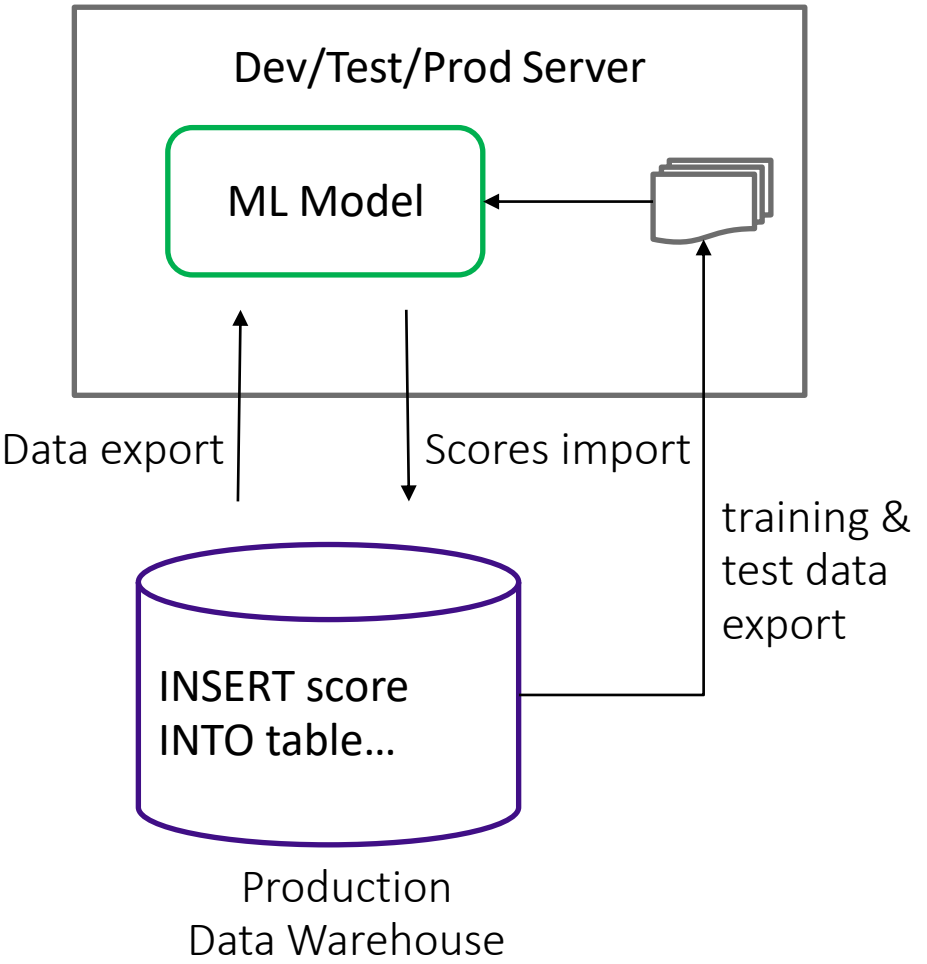


Several options available with different capabilities and objectives (e.g. Kubeflow, MLflow, Verta, SageMaker Model Registry).

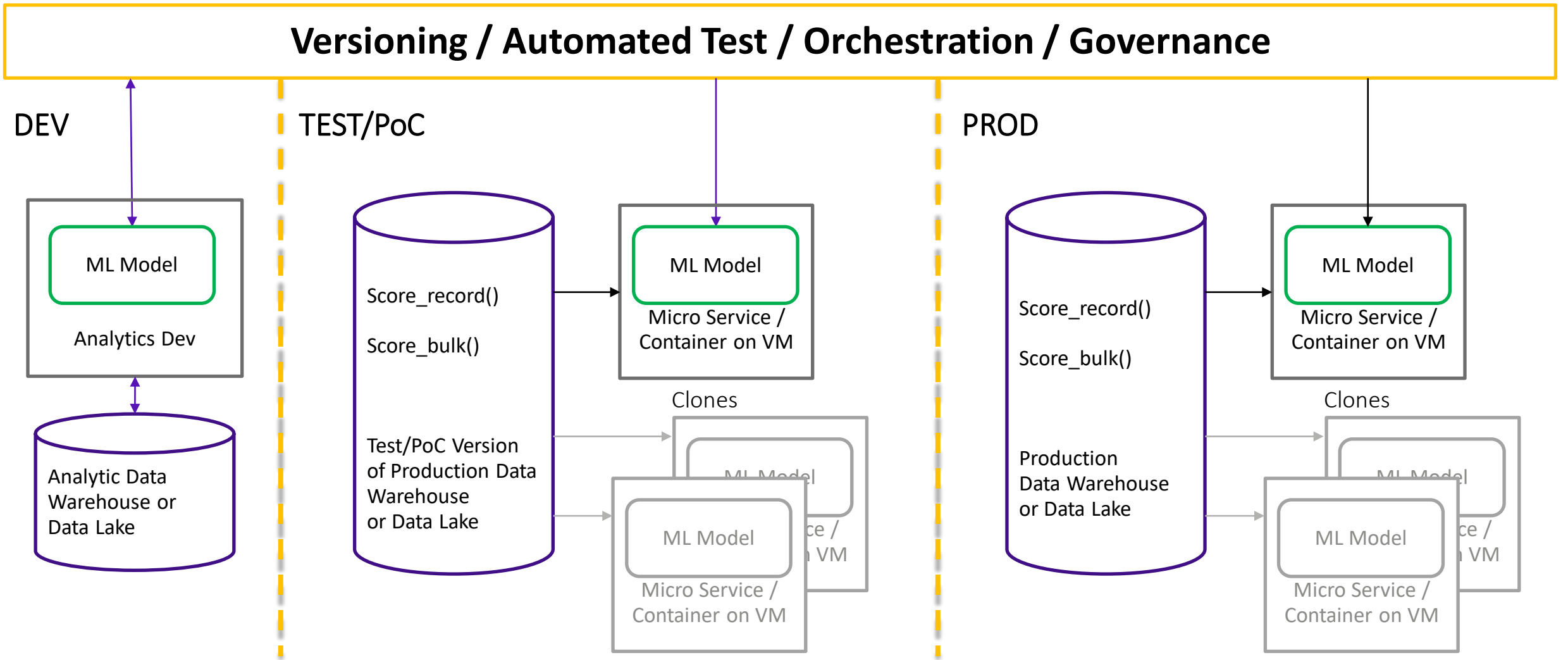
Developing into model pipeline/workflow managers.

Typical Use of ML Models – Lack of Efficiency, Governance & Rigor



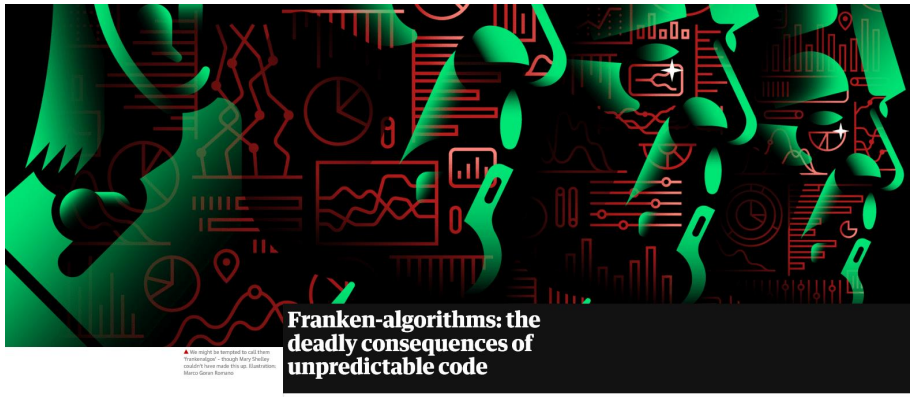


Better Model: Learn from Software Engineering



AI Governance – Manage Risks Across the AI Lifecycle

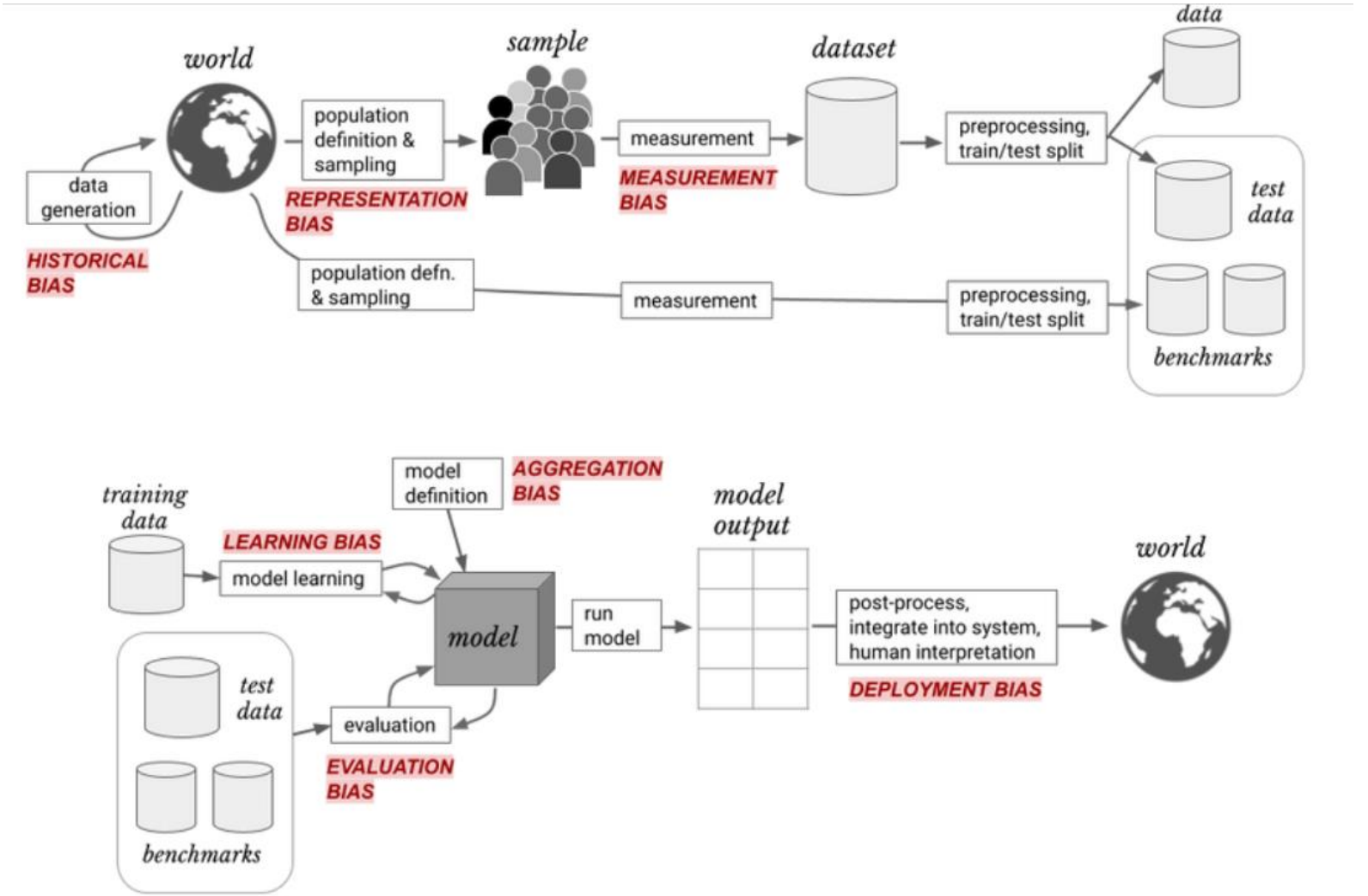
- Automated decision making – no human involved
- Statistical machine learning – can't foresee all possible outputs
- Training data – can't be certain about quality, completeness, errors, bias, …
- Scale of impact - AI amplifies risks in
  - Fairness (Bias)
  - Transparency
  - Reliability & Safety
  - Privacy & Security
  - Inclusivity
  - Accountability



https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger

IBM AI Fairness 360 Open Source Toolkit
(https://aif360.mybluemix.net/)

Sources of Harm in the Machine Learning Life Cycle



From: Harini Suresh and John Guttag: Understanding Potential Sources of Harm throughout the Machine Learning Life Cycle
https://mit-serc.pubpub.org/pub/potential-sources-of-harm-throughout-the-machine-learning-life-cycle/release/2

What is an ML model and how should it be managed?

- Code?

  It processes data and computes an output.

- Data?

  It is mainly defined by its parameters.

- Code & Data?

  It is an artefact created through a learning algorithm (code) from examples (data) resulting in a parameter configuration (data) that determines how to compute (code) new outputs.

- Data Product View

  How to do performance/QoE/usage monitoring? How to provide mitigation/insurance for wrong decisions?

From Model (Data Product) Build to Deployment and Beyond

Build (Development)

- Track data, metrics, parameters, and artefacts (features & models) as part of experiments
- Package models and reproducible ML projects (includes software environment)

Deploy (Commission)

- Deploy packaged models to batch or real-time serving platforms or old school to database
  (on Azure, Amazon, GCP, … as VM, Kubernetes cluster, docker container, microservice, serverless, …,
  or scheduled DB procedure, …)

Operate

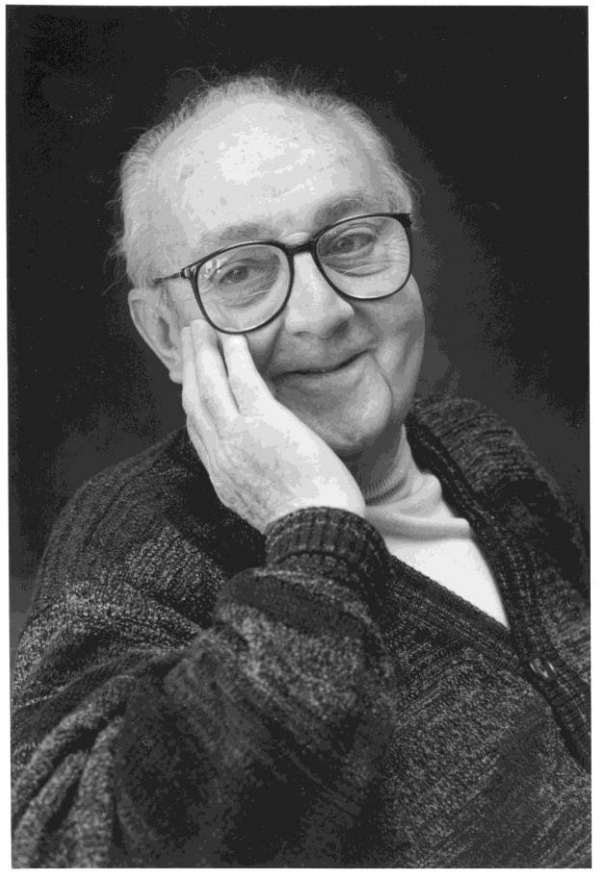
- Register and track models through their lifecycle
- Monitor data and features processed by the model
- Monitor models in production (record every decision they make, who uses them for what purpose, …)

Retire (Decommission)

- Archive models and their documented usage

Occam’s Razor

In science simpler theories are preferable to more complex ones because they are more testable



George Edward Pelham Box
(18 October 1919 – 28 March 2013)
British statistician

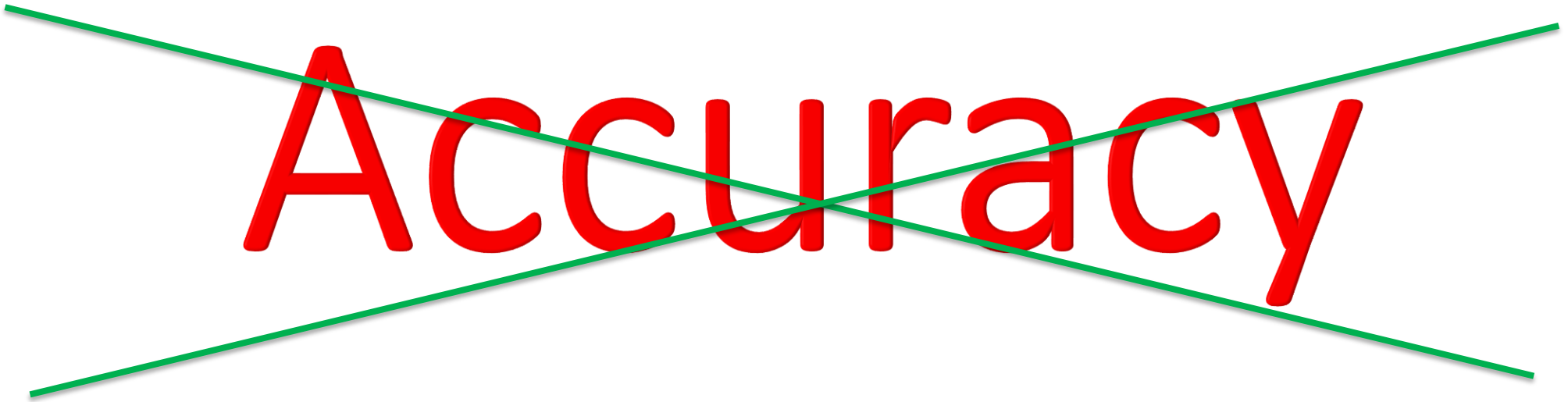
All models are wrong, but some are useful.

George E.P. Box, 1978

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

Since all models are wrong the scientist cannot obtain a "correct" one by excessive elaboration. On the contrary following William of Occam he should seek an economical description of natural phenomena. Just as the ability to devise simple but evocative models is the signature of the great scientist so overelaboration and overparameterization is often the mark of mediocrity.
George E.P. Box, 1976

The Most Misused Term in Data Science, AI & Machine Learning



Avoid using it!

The Accuracy of a Classifier (or the Base Rate Fallacy)

- Taken from the book “The Drunkards Walk: How Randomness Rules Our Lives” by Leonard Mlodinow.

- In 1989, the author’s application for life insurance was rejected because he tested positive for Aids. His doctor told him the he had a 999 out of 1000 chance to be “dead in a decade”.

- The author is still around, so what happened? Was he just really lucky? How did his doctor arrive at those odds?

Some background information

- In 1989, 1 in 10,000 male Americans from a non-at-risk group were infected with Aids (Centre for Disease Control and Prevention)
- The test produced a *false positive* result in 1 out 1000 tests (i.e. saying the patient has the Aids virus when they do not).
- The test has a *false negative* rate of near 0 (i.e. missing an infection when it is indeed present)

		Test says: Aids	Test says: No Aids
Patient has	Aids	TP=1/10,000	FN=0/10,000
	No Aids	FP=10/10,000	TN=9989/10,000

So what went on?

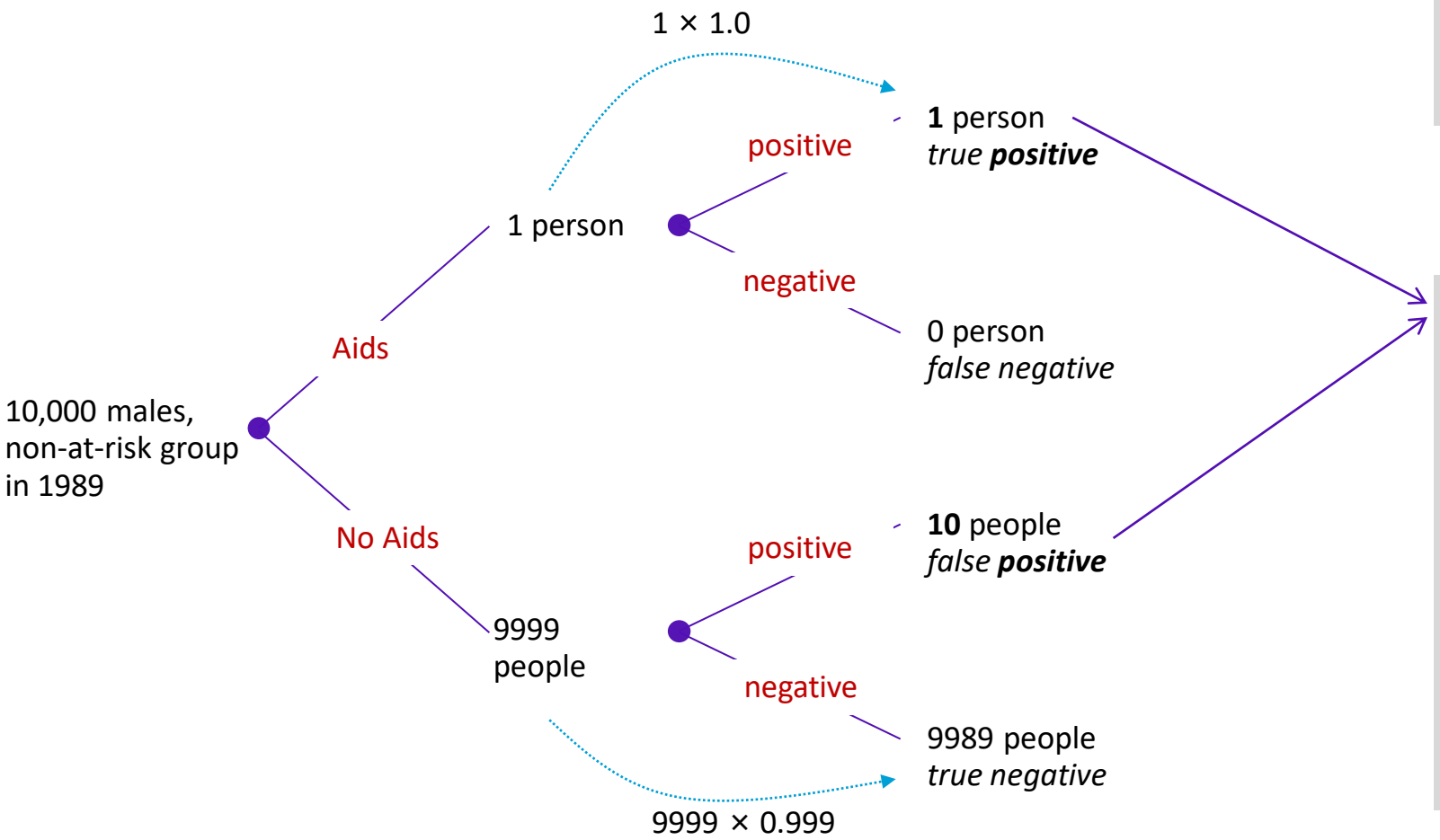
- The doctor mistook the *false positive rate* (fpr = 1/1000) for the chance that the test was wrong and that M. was in fact healthy. He computed 1-1/1000 = 999/1000 as M.'s chance of having Aids. (Since there are no false negatives in this case this is also the test accuracy).

- This is what he should have computed:
- Assume we test 10,000 people from a non-at-risk group.
- We will find 1 true positive and 10 false positives, i.e. 11 positives
- The other 9989 patients will test as true negatives.

- The real question to ask is: "What are the chances M. has Aids if the test result is positive"?
- The answer: only 1 in 11.

- It turned out the test was fooled by certain markers that were present although the virus was not

The Base Rate Fallacy Illustrated



Aids base rate **1 per 10,000**
Test Sensitivity **100%**
Test Specificity **99.9%**

1+10 people test ***positive***

But...
only 1 has Aids

So chance of Aids given a positive test is

1/11 = 9.1%

The Base Rate Fallacy: Avoid It by Using Bayes Rule

TP Rate = TP / (TP + FN)

Base Rate = (TP + FN) / N

$$P(being\ ill|positive\ test) = \frac{P(postive\ test|being\ ill)\ P(being\ ill)}{P(positive\ test)}$$

(TP + FP) / N

$$P(being\ ill|positive\ test) = \frac{1.0\ \cdot 0.0001}{0.0011} = 0.091$$

Precision = TP / (TP + FP)

Bookmark: https://en.wikipedia.org/wiki/Confusion_matrix

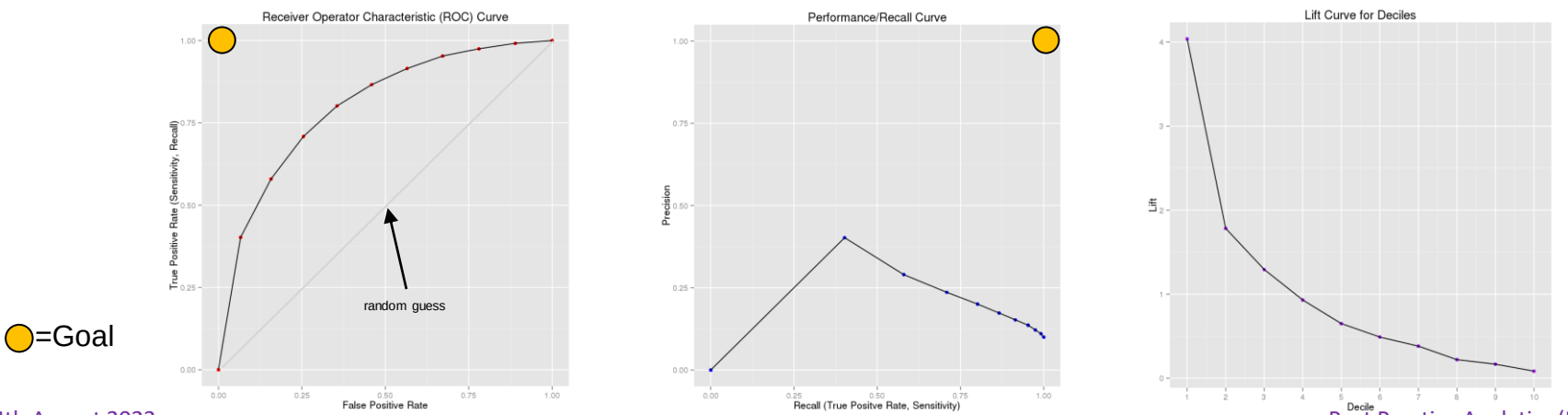
Understanding if a Predictive Model (Classifier) is Useful

- Just quoting the accuracy of a model can be misleading especially in cases where the data is extremely skewed and the target class is rare (e.g. crime, churn, fraud, faults, …).

  Example: if the churn probability is 1% then a model that classifies everyone as non-churner is 99% correct but 100% pointless.

- Ideally, we want to understand the trade-off between benefit and cost of a model which can be expressed in different ways depending on context.

- Always use cross-validation when building a model. Look at ROC, Performance/Recall, Lift Chart, Score Distribution, …



Making the Business Case for an AI Model

C:/Users/700714573/R/modelfactory/ModelCheck - Shiny

http://127.0.0.1:4036 | Open in Browser | Publish

Model Factory - Binary Classifier Evaluation Dashboard

Load data or model

Browse... ibm_churn_moc

Upload complete

Confidence level c to predict at:

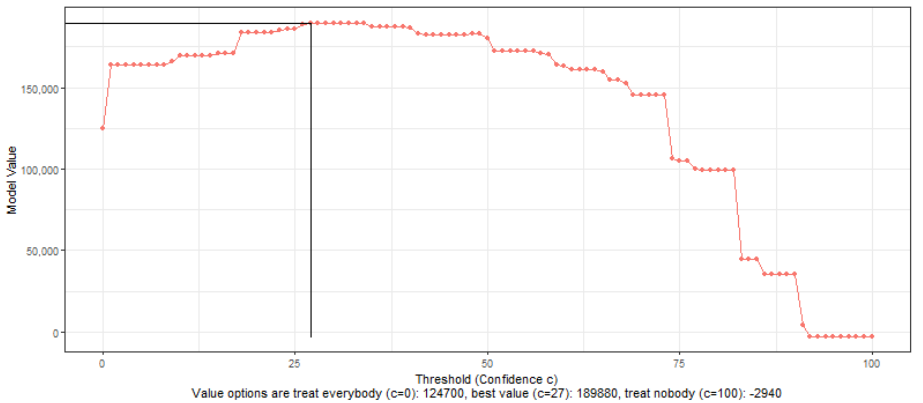
0 27 100

0 10 20 30 40 50 60 70 80 90 100

Evaluation

Generate report

ROC Plot | P-R Plot | Lift Plot | Value Plot | Score Distribution — Performance Plots



Value options are treat everybody (c=0): 124700, best value (c=27): 189880, treat nobody (c=100): -2940

Confusion Matrix

	Actual 0	Actual 1
Predicted 0	758	26
Predicted 1	795	534

Statistics

- Data loaded from file: ibm_churn_model.rds
- Base rate of positive class 1: 26.5%
- Predicted scores are in range [0, 1]
- AUC: 0.84

Model Value | Model CE Impact — Model Value and Customer Experience

Specify a benefit as a positive value and a cost as a negative value.

Value of a True Negative: 10

Cost of a False Negative: -200

Cost of a False Positive: -100

Value of a True Positive: 500

Model Value Matrix

	Actual 0	Actual 1
Predicted 0	7580.00	-5200.00
Predicted 1	-79500.00	267000.00

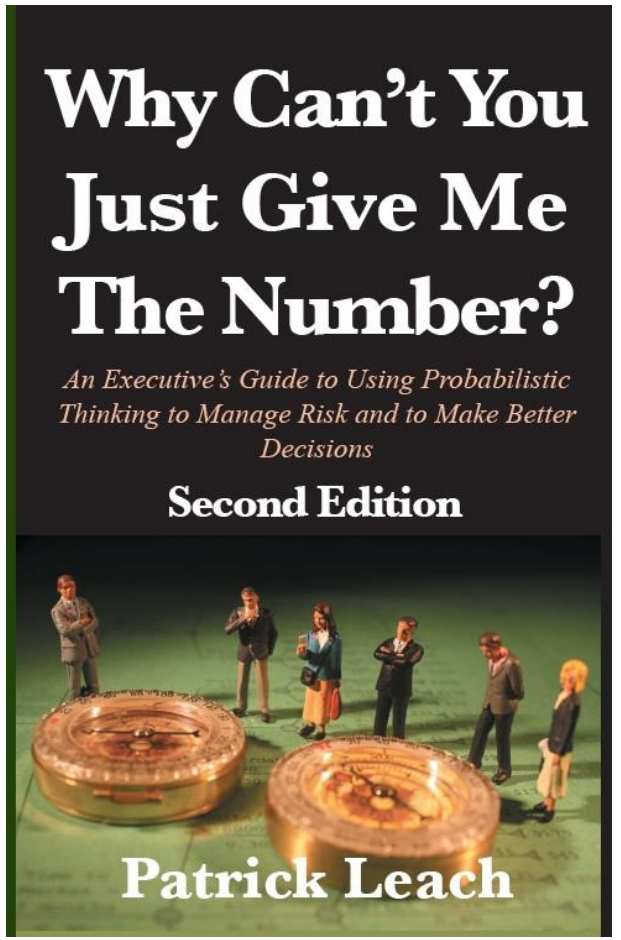
Average Expected CE Changes

	Actual 0	Actual 1
Predicted 0	0.00	0.00
Predicted 1	0.00	0.00

189,880
Total Model Value

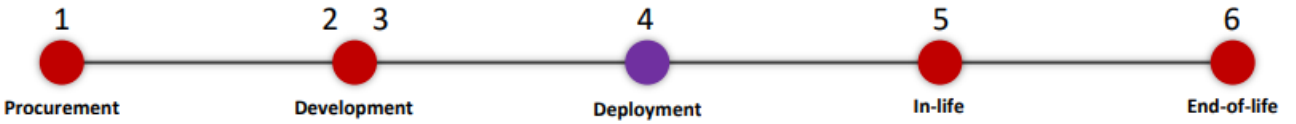
0
Average CE Change

Decision Making Based on Analytics



- Executives are not necessarily familiar with analytics
- Analysts can find it difficult to present results as compelling business cases and explain risks
- Managers must become comfortable with systematic experimentation with rigorous controls to determine cause and effect.
- Use prescriptive analytics: say what to do with the outcome and explain risks and contingencies
- Closely monitor deployments

AI Checklists



AI DEPLOYMENT

1. Stakeholders identified and engaged[q]
2. Confirm development history is preserved[q]
3. Confirm all testing has been completed
4. Confirm AI operational warranty is in place and is consistent with planned deployment[r].
5. Define and agree AI model contract and ensure this is enforceable[s].
6. Where appropriate, ensure a model fail-safe mechanism is in place[t].
7. Establish end-of-life plan[u]
8. Verify that the planned deployment is aligned with organisational AI policy.
9. Confirm all regulatory considerations on data access, privacy and geographic restrictions on where systems and data can be run or moved have been addressed.

AI DELPOYMENT – guidance

[q] **Development history** All elements necessary to reproduce the system should be stored and discoverable based on the identity of the system to be deployed. Test plans and results should also be preserved so it can be understood what aspects of the systems were tested and how it performed.

[r] **AI warranty** The planned deployment should be consistent with the limits and constraints declared in the AI operational warranty. If this is not the case, mitigating actions to manage the risks should be in place and documented.

[s] **AI model contract** A 'contract' identifying dependencies and constraints for the safe and correct operation of the AI system should be in place. The system implementation should provide the means to validate and enforce the contract (eg by supporting the TM Forum AI Management APIs).

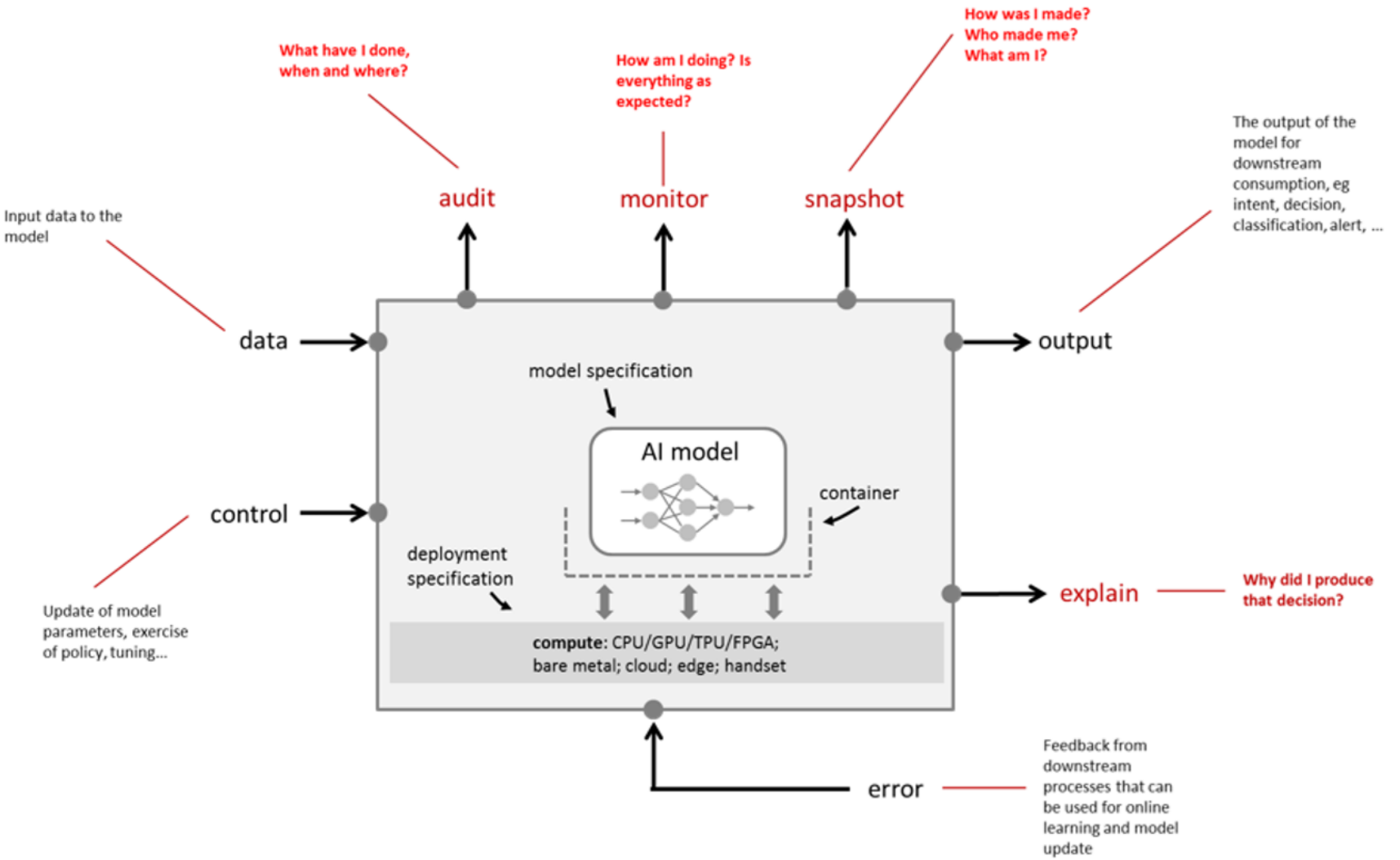
[t] **Fail-safe** Where the model can mobilize resources independently, measures need to be developed to stop a potential runaway.

[u] **End-of-life plan** The end-of-life requirements for this system should be documented prior to deployment. This should identify retention periods for all historical information relating to the system (eg development history, chain-of-custody, audit logs).

tmforum

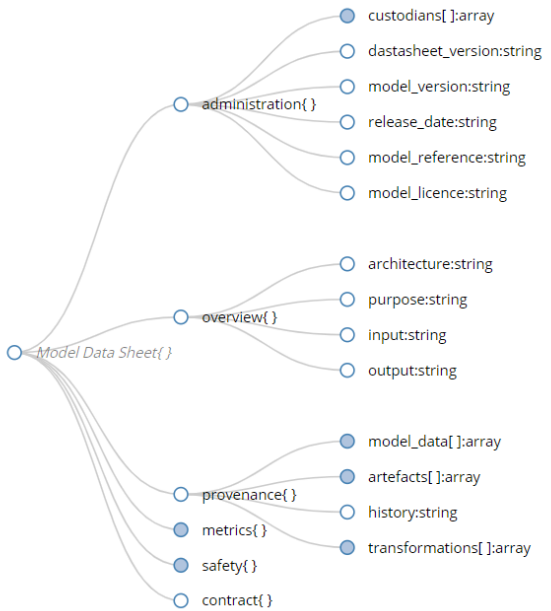
BT

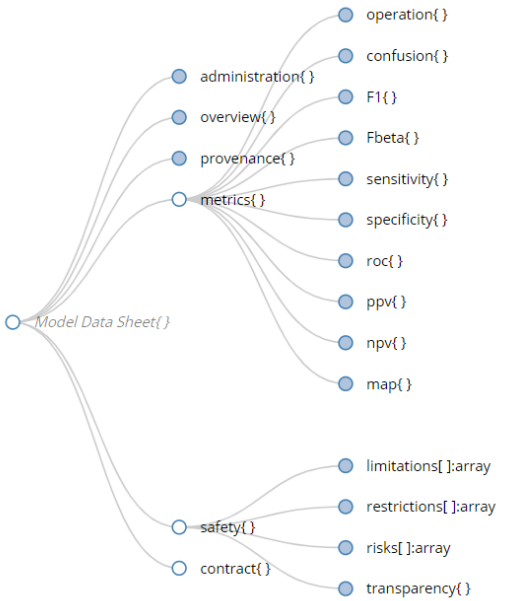
High Level Model for AI Management



TM Forum Standard: Service Management Standards for AI. IG1184, Release 18.5.1, Feb 2019.

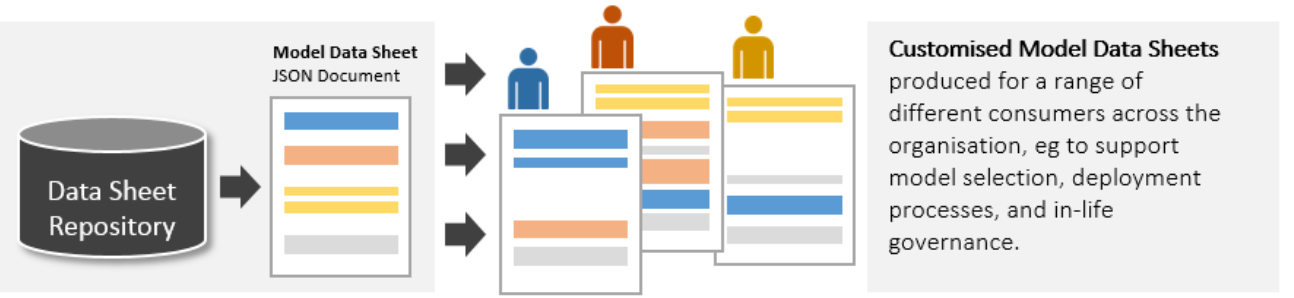
Model Data Sheets





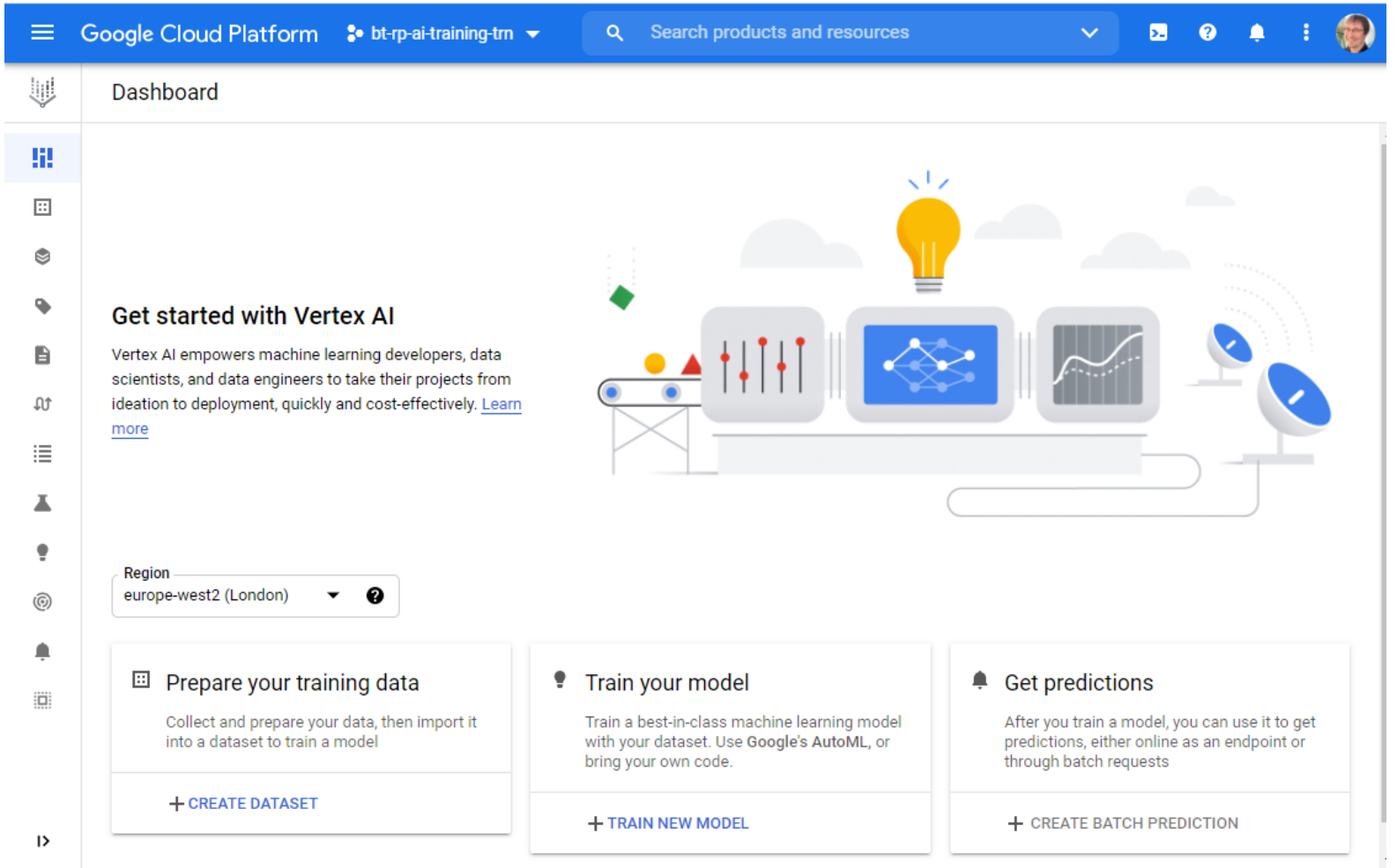
Populating the Model Data Sheet

Consuming the Model Data Sheet



tmforum

The New AI/ML Landscape: AutoML and MLOps



MLOps?

MLOps: General idea is DevOps applied to Machine Learning

DevOps: Continuous development practice in software engineering.

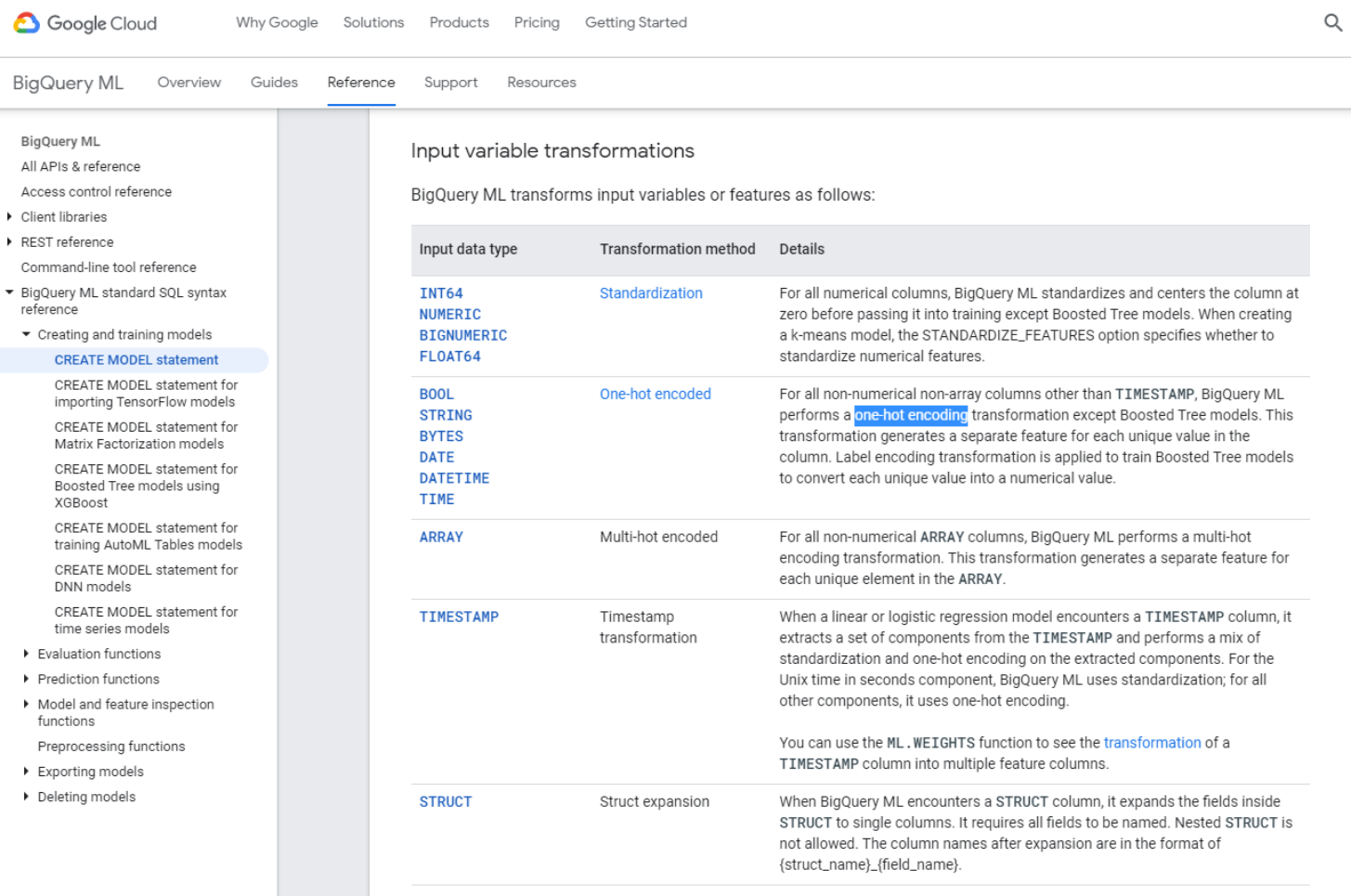
You can also call it *Production Machine Learning*

MLOps - Wikipedia

- *MLOps is the process of taking an experimental Machine Learning model into a production system.*
- *Goals:*
  - *Deployment and automation*
  - *Reproducibility of models and predictions*
  - *Diagnostics*
  - *Governance and regulatory compliance*
  - *Scalability*
  - *Collaboration*
  - *Business uses*
  - *Monitoring and management*

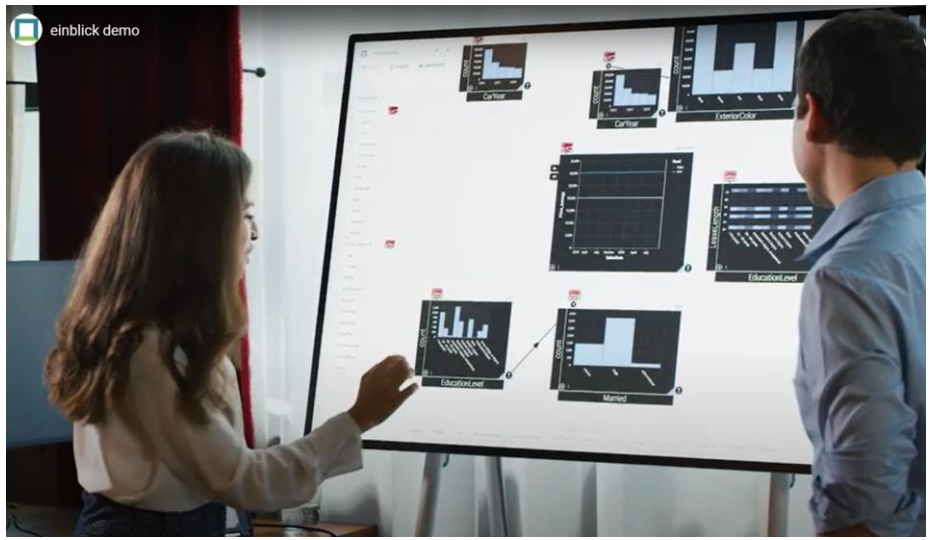
Trend: Cloud providers are making ML available as part of Query Languages

- These ad-hoc models are not tracked for monitored for quality.
- Targets a user community (data engineers and data analysts) who may have a lack of understanding how to use ML.
- To work in queries ML engines need to make a lot of assumptions. Users may not be aware of the impact.
- Example: Team at a hackathon was attempting to build a text classifier. The ML engine used default one hot encoding across all text samples.
- **Democratisation of ML needs guardrails.**



Trend: Collaborative Visual Data Analysis with AutoML

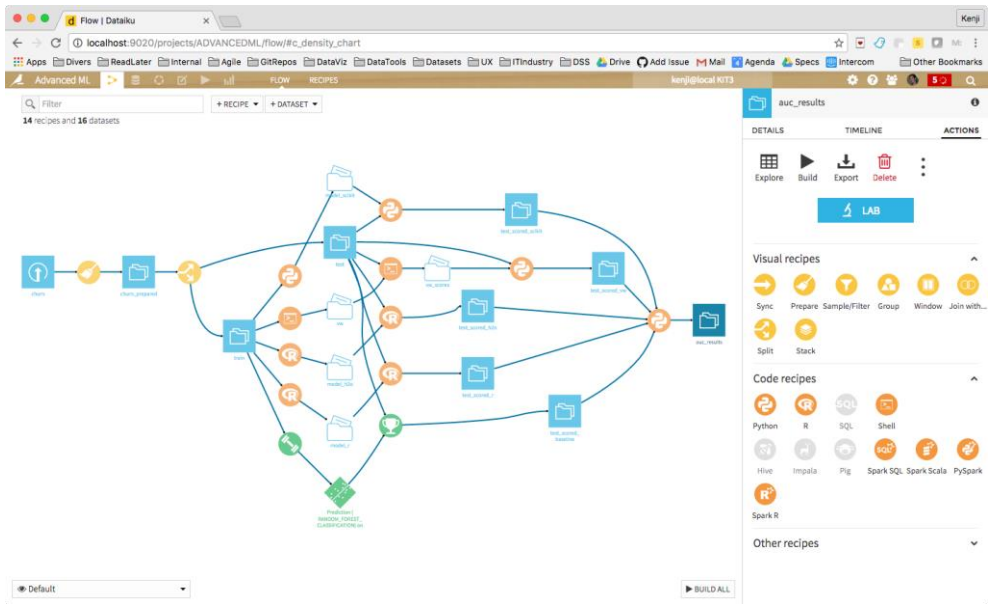
- Einblick Analytics is a start-up out of MIT
- The tool is positioned as a visual data computing platform
- Intuitive, collaborative UI, AutoML with guardrails, but not for ML development
- Targets teams and non-experts
- Has guardrails to constrain ML.

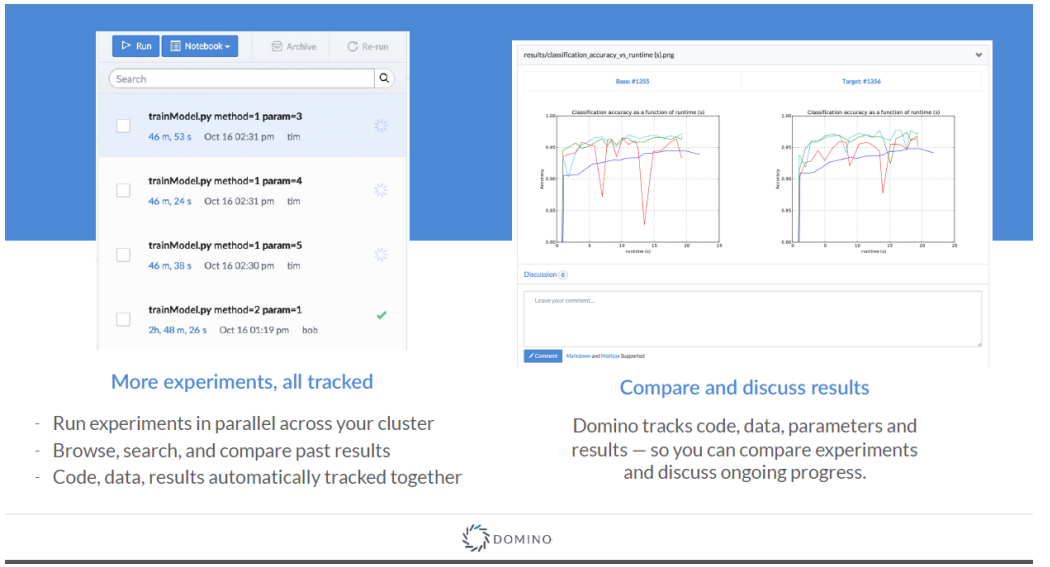


https://einblick.ai

Now Standard: Versioning and Collaboration

Dataiku – Integrated environment with versioning, collaboration and deployment (http://dataiku.com)

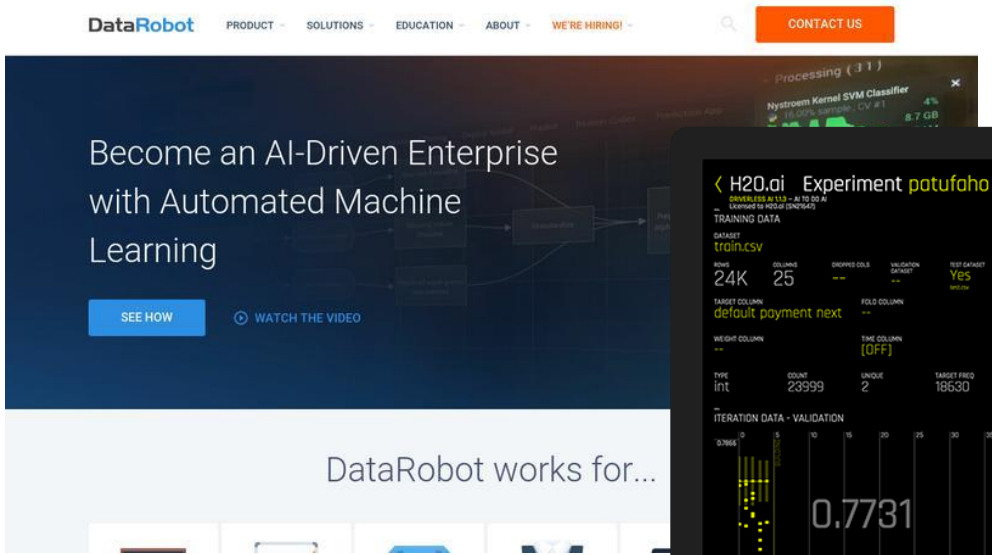




Domino – cloud based environment for analytics (Notebooks, RStudio), versioning, collaboration, and deployment (http://dominodatalabs.com)

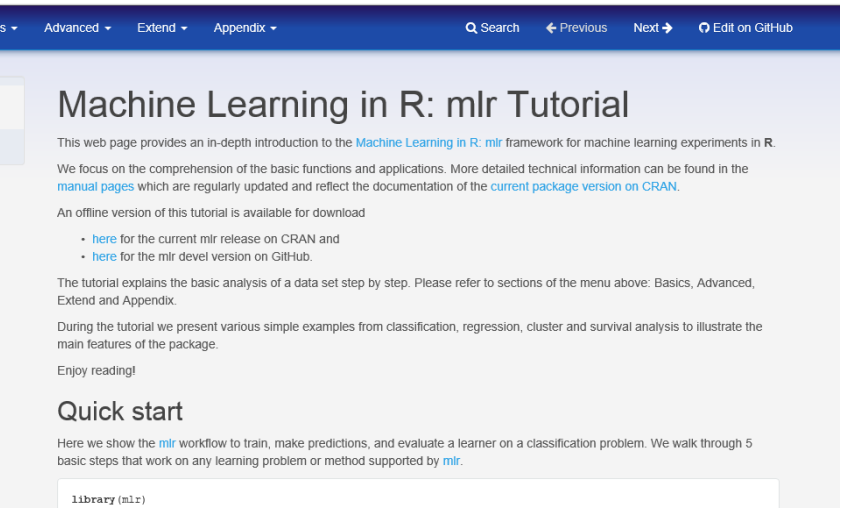
Now Standard: Automated Modelling

Fully automated environments – e.g. DataRobot …

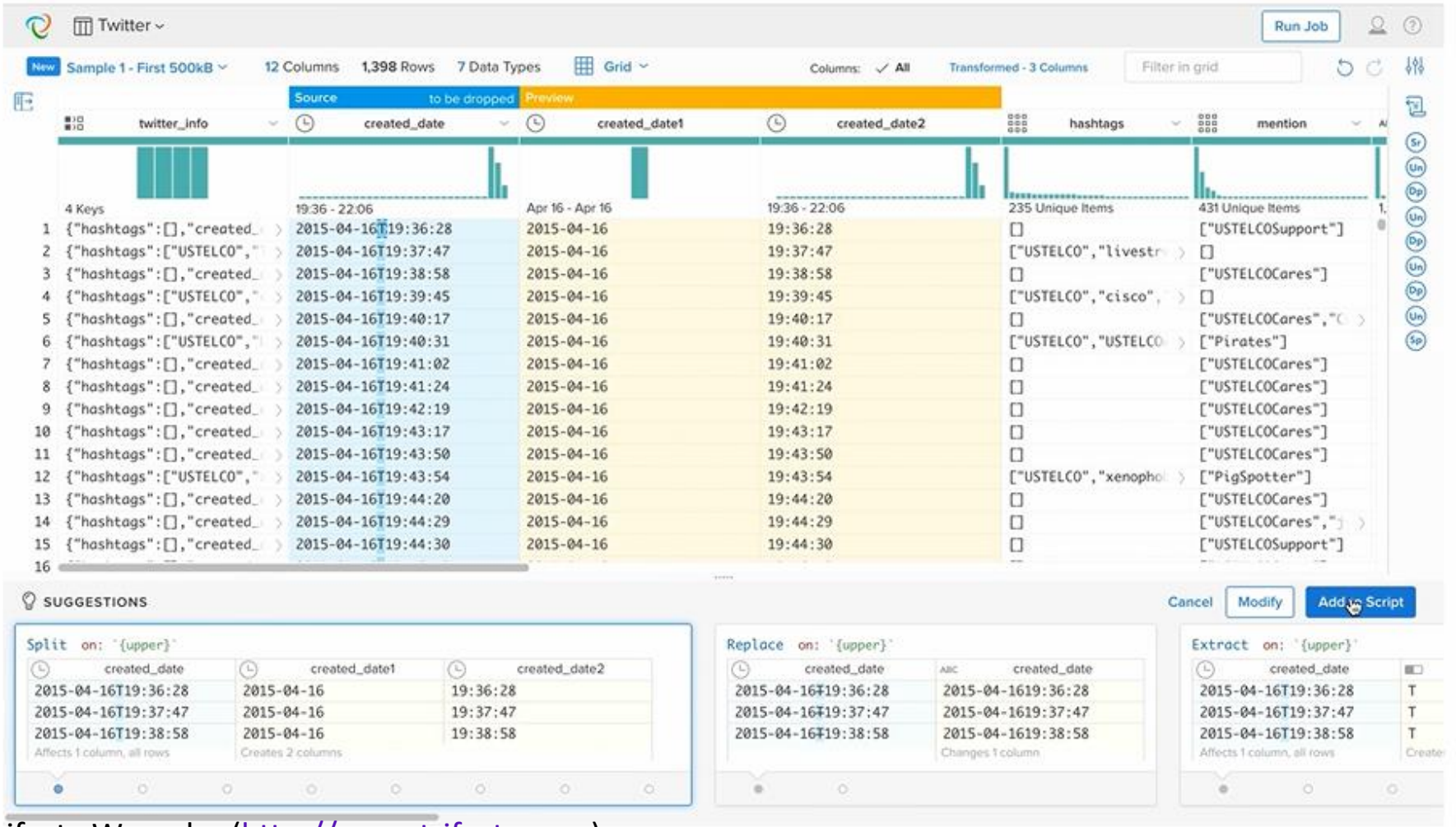


… or H2O Driverless AI

Libraries for R and Python providing a unified API and semi-automation (e.g. MLR, SciKit Learn)



Data Wrangling – Some Semi-Automated Tools Exist



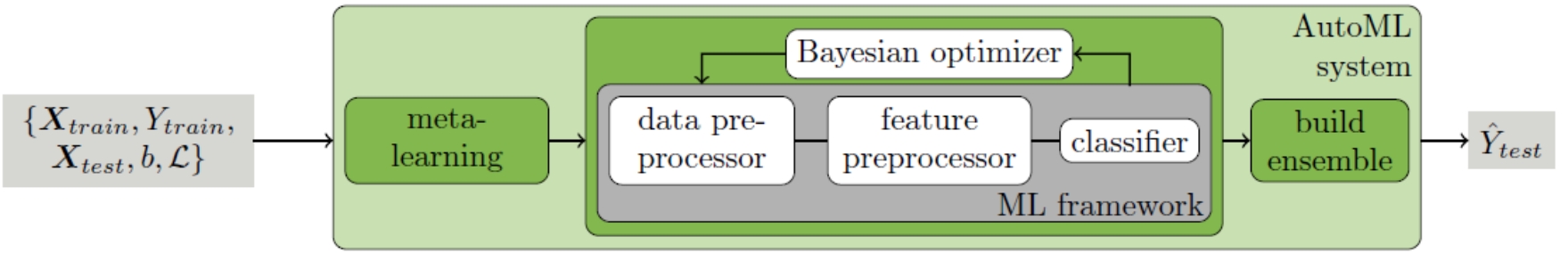
Trifacta Wrangler (http://www.trifacta.com)

Automated Machine Learning

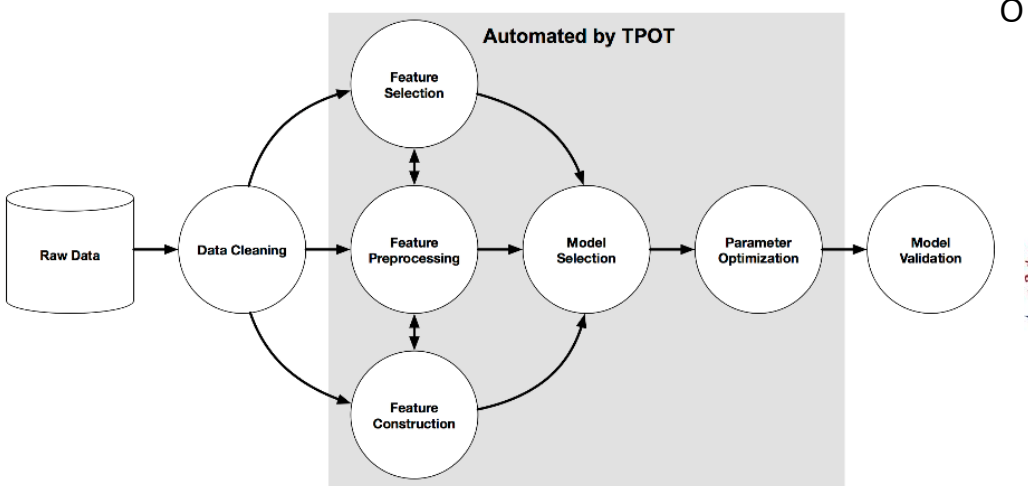
Different approaches exist:

- Find best hyper-parameters for ML algorithms through optimisation strategies.
- Create a grammar of models and use graph-based search.
- Combine data pre-processing and ML operators into workflows e.g. through genetic programming

AutoML for Python (based on scikit-learn)



Auto-sklearn: Bayesian optimisation for hyper-parameter optimisation



TPOT: uses genetic programming to test combinations of feature representations, algorithms and hyper-parameters. Produces a pipeline of the best performing solution.

AutoML for R

`R packages`

- `caret` (by Max Kuhn, http://topepo.github.io/caret/)
- `mlr3` (https://mlr3.mlr-org.com/)
- `tidymodels` (https://www.tidymodels.org/)

The packages provide simplified usage of several ML algorithms

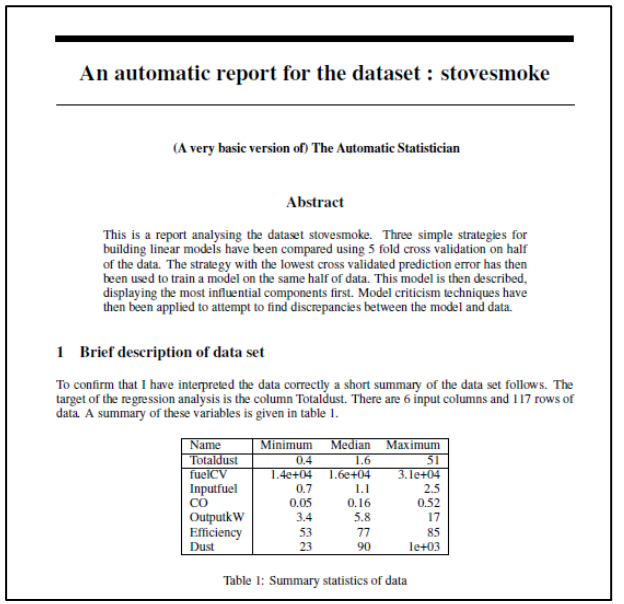
They offer hyper-parameter optimisation based on grid search and resampling, mlr3 also offers F-racing and model-based (Bayesian) optimisation.

mlr3 and tidymodels have a pipelines/workflow approach

The Automatic Statistician

(Zoubin Gharamani's group, Cambridge, www.automaticstatistician.com)

- Idea:
- have a language that can describe arbitrarily complicated models
- a method to search over those models
- a procedure to check model fit
- So far:
  Implementation for a grammar of Gaussian Processes which can be used for Bayesian Regression.
- Generates natural language report.



An automatic report for the dataset : stovesmoke

(A very basic version of) The Automatic Statistician

Abstract

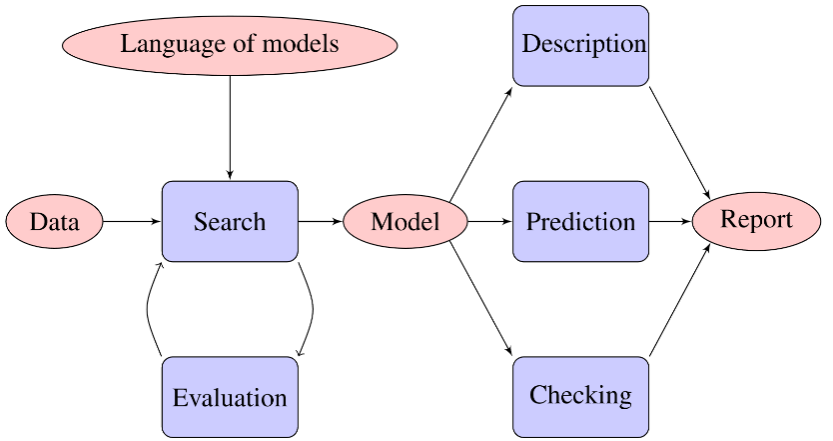
This is a report analysing the dataset stovesmoke. Three simple strategies for building linear models have been compared using 5 fold cross validation on half of the data. The strategy with the lowest cross validated prediction error has then been used to train a model on the same half of data. This model is then described, displaying the most influential components first. Model criticism techniques have then been applied to attempt to find discrepancies between the model and data.

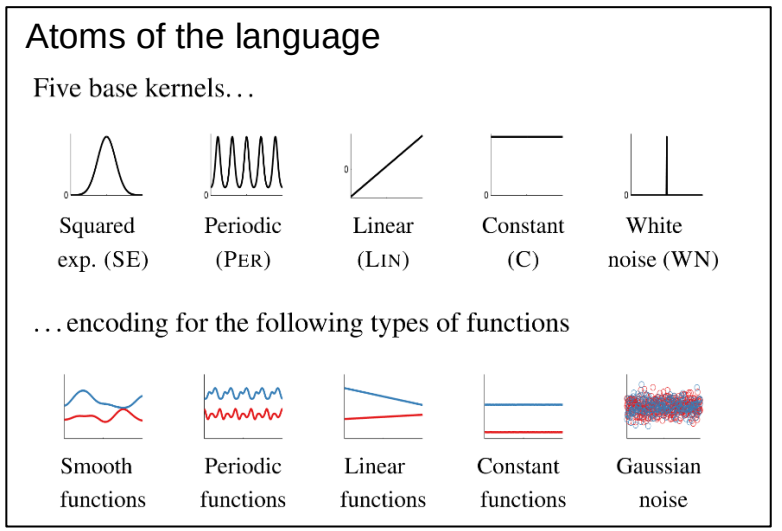
1 Brief description of data set

To confirm that I have interpreted the data correctly a short summary of the data set follows. The target of the regression analysis is the column Totaldust. There are 6 input columns and 117 rows of data. A summary of these variables is given in table 1.

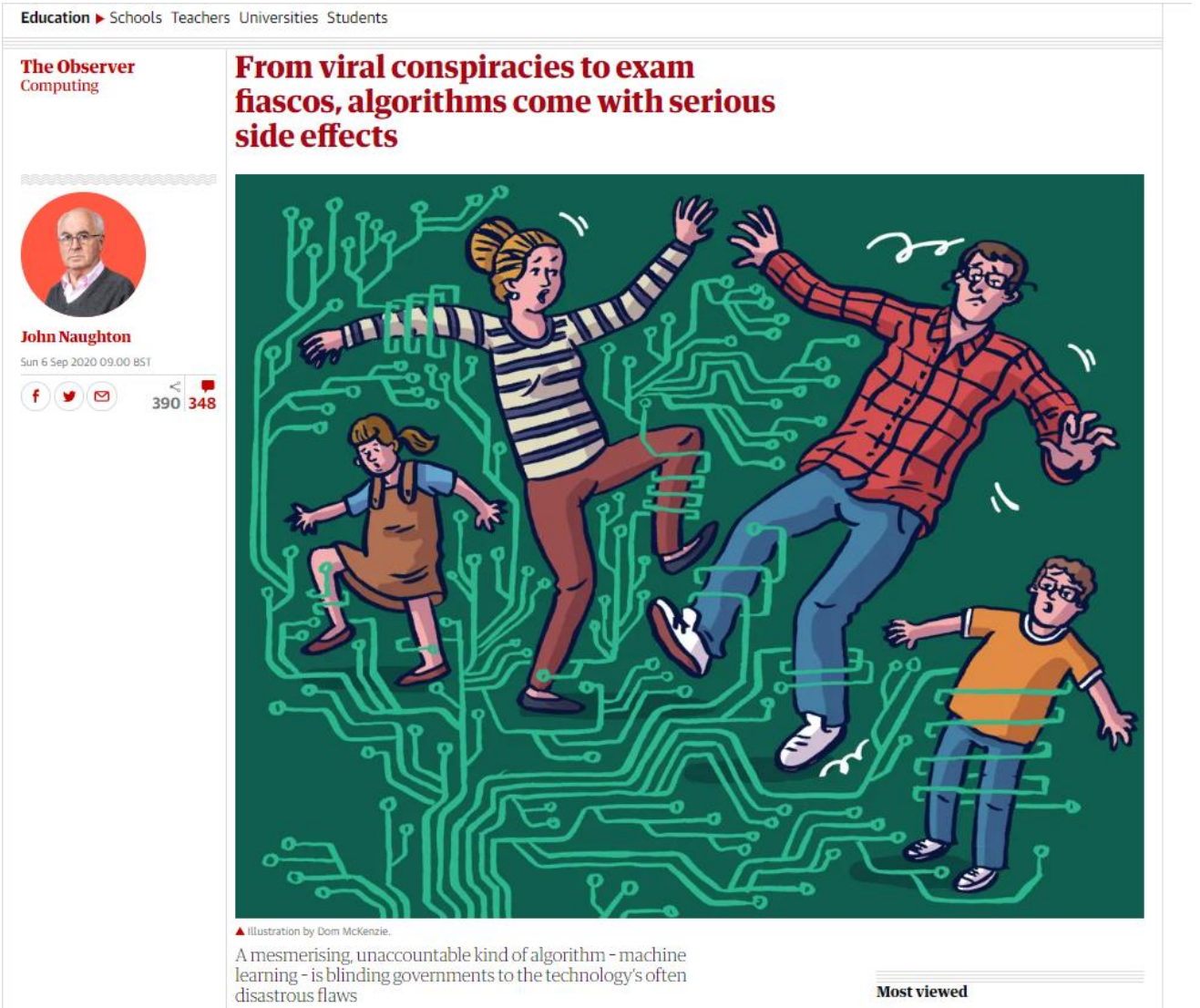
Name	Minimum	Median	Maximum
Totaldust	0.4	1.6	51
fuelCV	1.4e+04	1.6e+04	3.1e+04
Inputfuel	0.7	1.1	2.5
CO	0.05	0.16	0.52
OutputkW	3.4	5.8	17
Efficiency	53	77	85
Dust	23	90	1e+03

Table 1: Summary statistics of data





“Algorithms” in the Public Eye



Education ▸ Schools Teachers Universities Students

The Observer
Computing

From viral conspiracies to exam fiascos, algorithms come with serious side effects

John Naughton

Sun 6 Sep 2020 09.00 BST

390 348

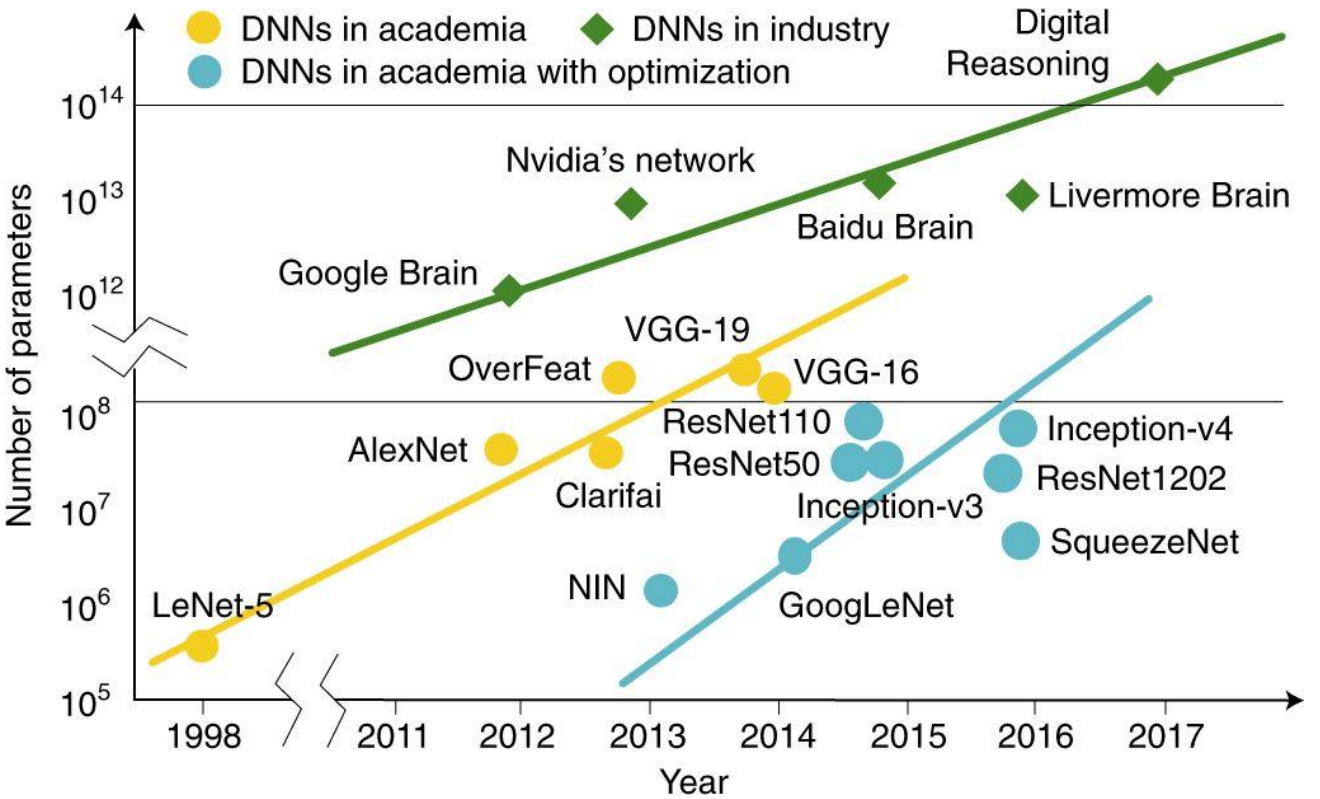
▲ Illustration by Dom McKenzie.

A mesmerising, unaccountable kind of algorithm - machine learning - is blinding governments to the technology's often disastrous flaws

Most viewed

https://www.theguardian.com/technology/2020/sep/06/from-viral-conspiracies-to-exam-fiascos-algorithms-come-with-serious-side-effects

Sizes of Neural Network Architectures Are Growing Exponentially



Xu, X., Ding, Y., Hu, S.X. *et al.* Scaling for edge inference of deep neural networks. *Nat Electron* **1,** 216–222 (2018). https://doi.org/10.1038/s41928-018-0059-3

This is becoming unsustainable fast – e.g. BERT network for language translation (110m parameters): Building it was $4K – $12K for cloud compute cost and the carbon equivalent of a flight from NY to SF*. The GPT-3 model, an autoregressive language model, uses 175 billion parameters and training it required almost 2,000 times more compute effort than BERT† (carbon equivalent not available).

*

Emma Strubell, Ananya Ganesh, Andrew McCallum:
Energy and Policy Considerations for Deep Learning in NLP.
College of Information and Computer Sciences, University of Massachusetts Amherst.
https://drive.google.com/file/d/1v3TxkqPuzvRfiV_RVyRTTFbHl1pZq7Ab/view

†

Tom B. Brown et al: Language Models are Few Shot Learners. Open AI, 2020.
https://arxiv.org/pdf/2005.14165.pdf

The Gradient

HOME OVERVIEWS PERSPECTIVES ABOUT SUBSCRIBE CONTRIBUTE

Shortcuts: How Neural Networks Love to Cheat

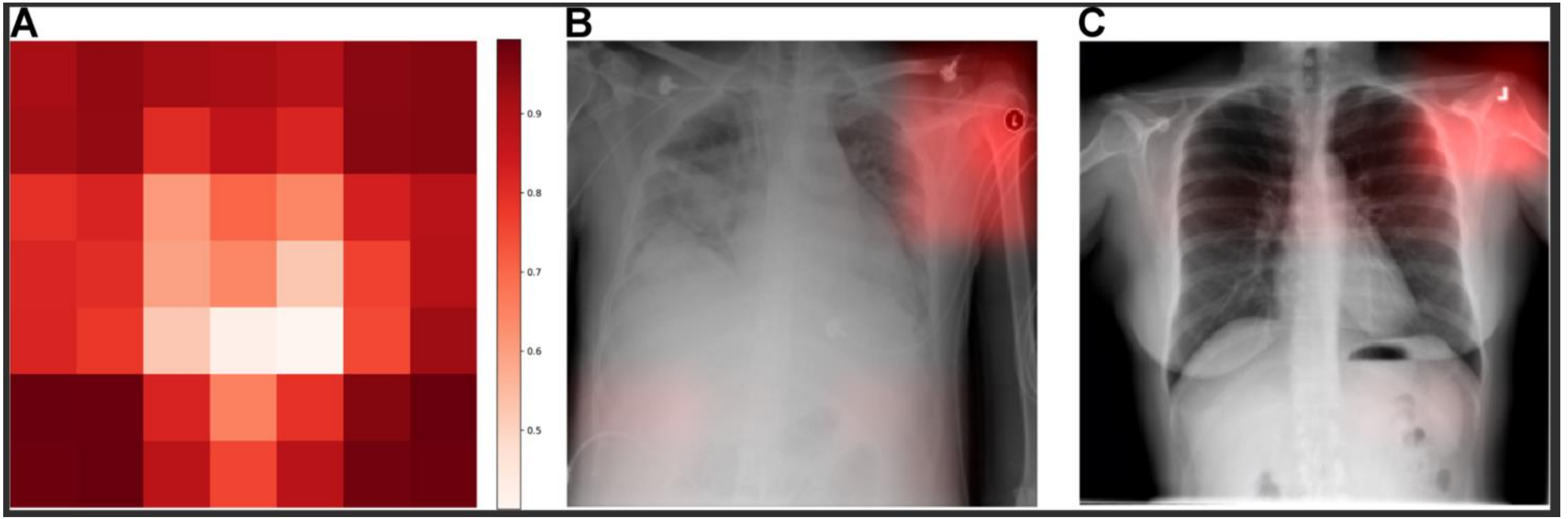
25.JUL.2020

Jörn-Henrik Jacobsen, Robert Geirhos, Claudio Michaelis

Will Artificial Intelligence soon replace radiologists? Recently, researchers trained a deep neural network to classify breast cancer, achieving a performance of 85%. When used in

Model cheating – sometimes it just does not work outside the lab

A: strongest contributions come from image corners. B/C: AI learnt to associate token with disease prevalence instead of diagnosing the x-ray image. It is important to check if the AI has focussed on artefacts or the features we want it to use.



Source: Variable generalization performance of a deep learning model to detect pneumonia in chest radiographs: A cross-sectional study | PLOS Medicine

Responsible AI: Guarantee Fairness – Avoid Bias

REUTERS World Business Markets Politics TV

Midterm Elections | Imprisoned In Myanmar | Sectors Up Close | Breakingviews | Investing | Future of Money | Charged:

Ad closed by Google

Stop seeing this ad | Why this ad?

BUSINESS NEWS OCTOBER 10, 2018 / 4:12 AM / A MONTH AGO

Amazon scraps secret AI recruiting tool that showed bias against women

Jeffrey Dastin 8 MIN READ

SAN FRANCISCO (Reuters) - Amazon.com Inc's (AMZN.O) machine-learning specialists uncovered a big problem: their new recruiting engine did not like women.

https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

TOM SIMONITE BUSINESS 03.29.18 07:00 AM

HOW CODERS ARE FIGHTING BIAS IN FACIAL RECOGNITION SOFTWARE

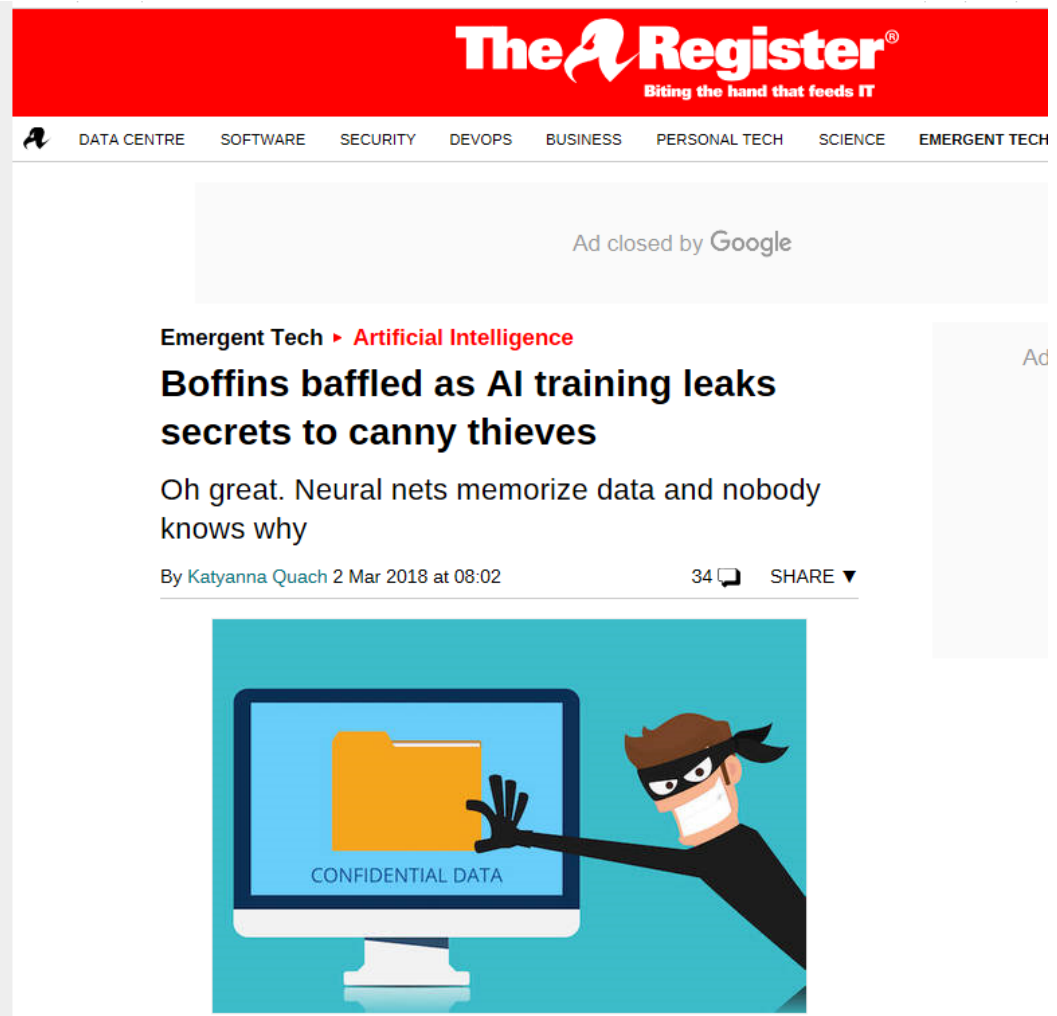
https://www.wired.com/story/how-coders-are-fighting-bias-in-facial-recognition-software/

Joy Buolamwini: “AI, Ain’t I a Woman?”

Joy Buolamwini did important influential work with her Gender Shades study demonstrating the gender and racial bias in facial image recognition software.

The Coded Gaze: Unpacking Biases in Algorithms That Perpetuate Inequity
https://www.rockefellerfoundation.org/case-study/unpacking-biases-in-algorithms-that-perpetuate-inequity/

Responsible AI: Privacy (Information Leakage)



The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE SECURITY DEVOPS BUSINESS PERSONAL TECH SCIENCE EMERGENT TECH

Ad closed by Google

Emergent Tech ▸ Artificial Intelligence

Boffins baffled as AI training leaks secrets to canny thieves

Oh great. Neural nets memorize data and nobody knows why

By Katyanna Quach 2 Mar 2018 at 08:02 34 SHARE ▼

https://www.theregister.co.uk/2018/03/02/secrets_fed_into_ai_models_as_training_data_can_be_stolen/

Nicholas Carlini, Chang Liu, Úlfar Erlingsson, Jernej Kos, Dawn Song:
The Secret Sharer: Evaluating and Testing Unintended Memorization in Neural Networks
https://arxiv.org/abs/1802.08232

Responsible AI: Transparency and Accountability

The Guardian view Columnists Cartoons Opinion videos Letters

Opinion
Artificial intelligence (AI)

We hold people with power to account. Why not algorithms?

Hannah Fry

Mon 17 Sep 2018 06.00 BST

495 581

As we delegate technology more responsibility to diagnose illness or identify suspects, we must regulate it

▲ 'All around us, algorithms provide a convenient source of authority; a short cut we take without thinking.' Photograph: Getty Images

https://www.theguardian.com/commentisfree/2018/sep/17/power-algorithms-technology-regulate

ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken | About the ICO

About the ICO / ICO and stakeholder consultations /

ICO consultation on the draft AI auditing framework guidance for organisations

Consultation Start Date **19 February 2020**
Type **ICO consultation, Open**

This consultation closes on 01 April 2020;

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/02/ico-consultation-on-the-draft-ai-auditing-framework-guidance-for-organisations/

Why Explanations from AI Systems?

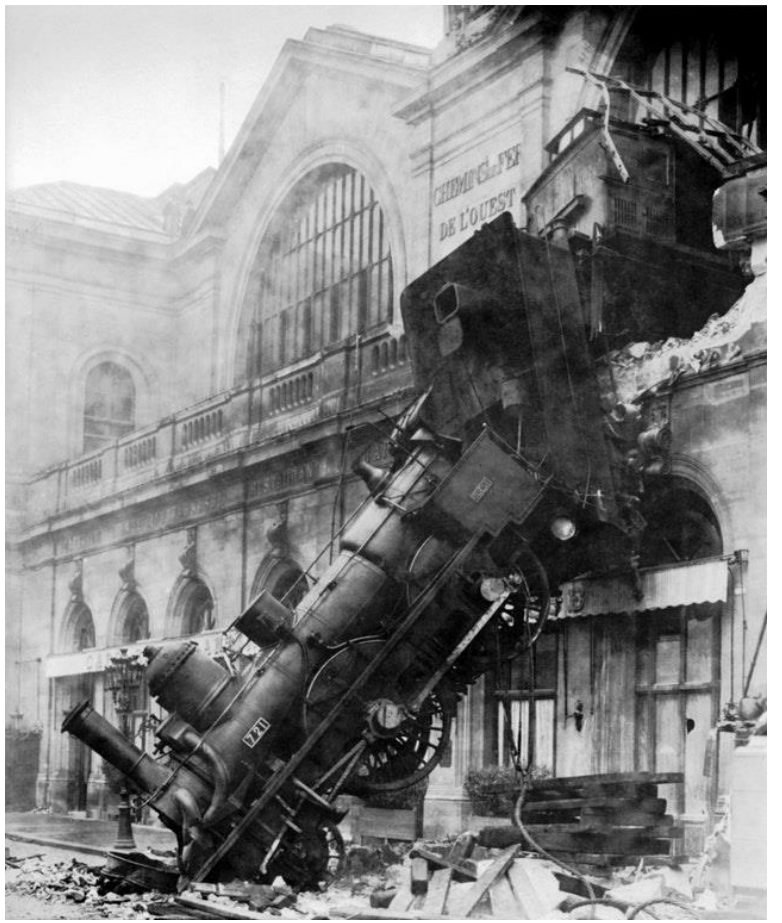
Good science, trust, causality

Ethics and fairness – is there bias?

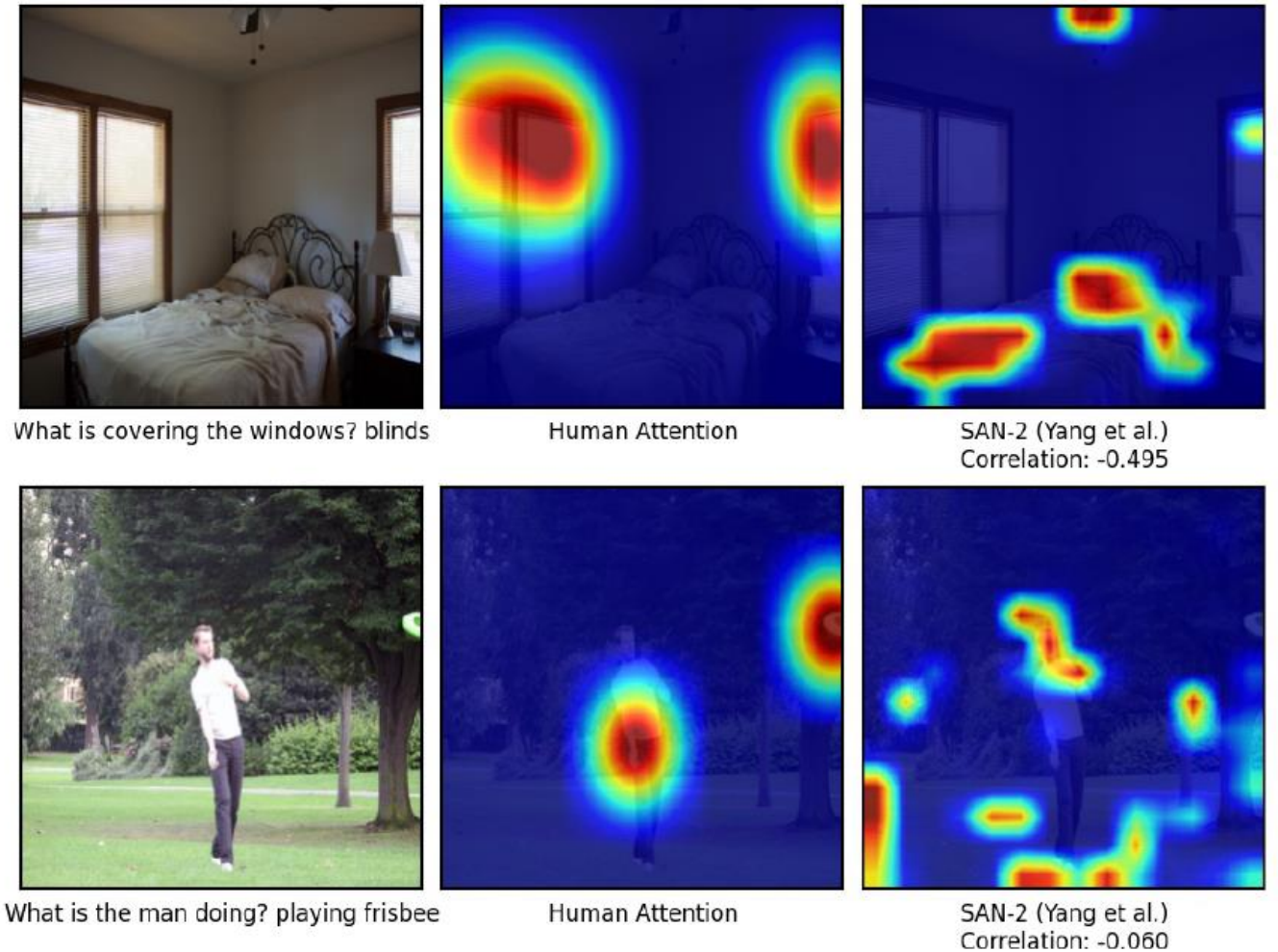
Challenge outcome of decisions

Legal and regulatory obligation

Learning from failure



Not all “explanations” are helpful



Source: Abhishek Das, Harsh Agrawal, C. Lawrence Zitnick, Devi Parikh, Dhruv Batra: Human Attention in Visual Question Answering: Do Humans and Deep Networks Look at the Same Regions, 2016 (https://arxiv.org/abs/1606.03556)

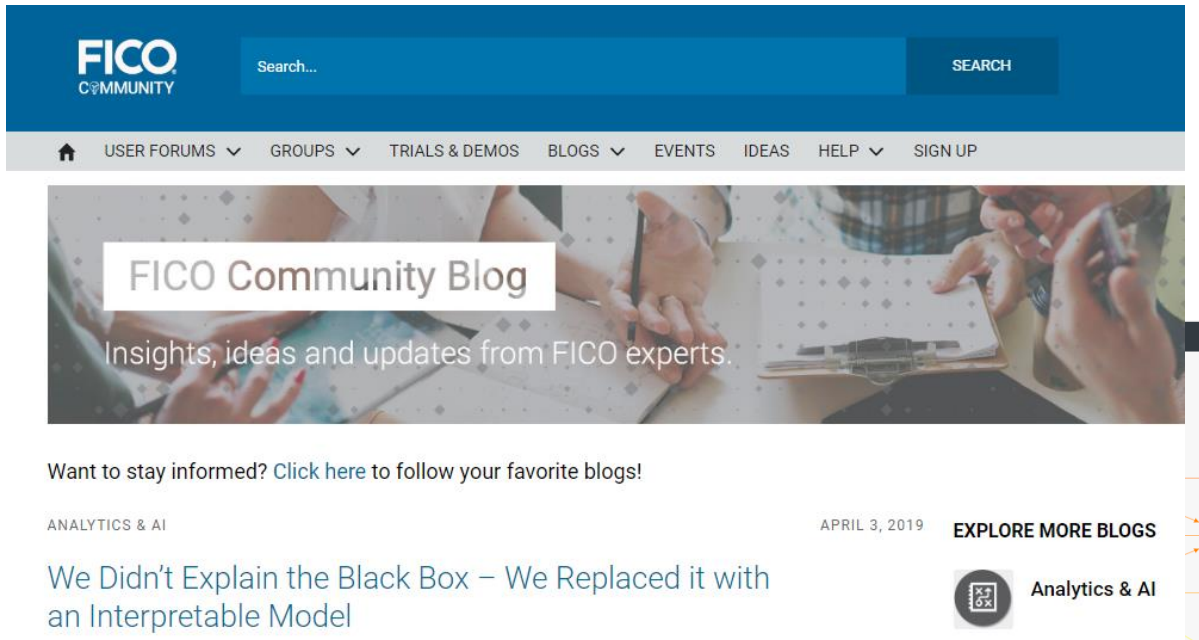
Explainable to / Interpretable by Whom?

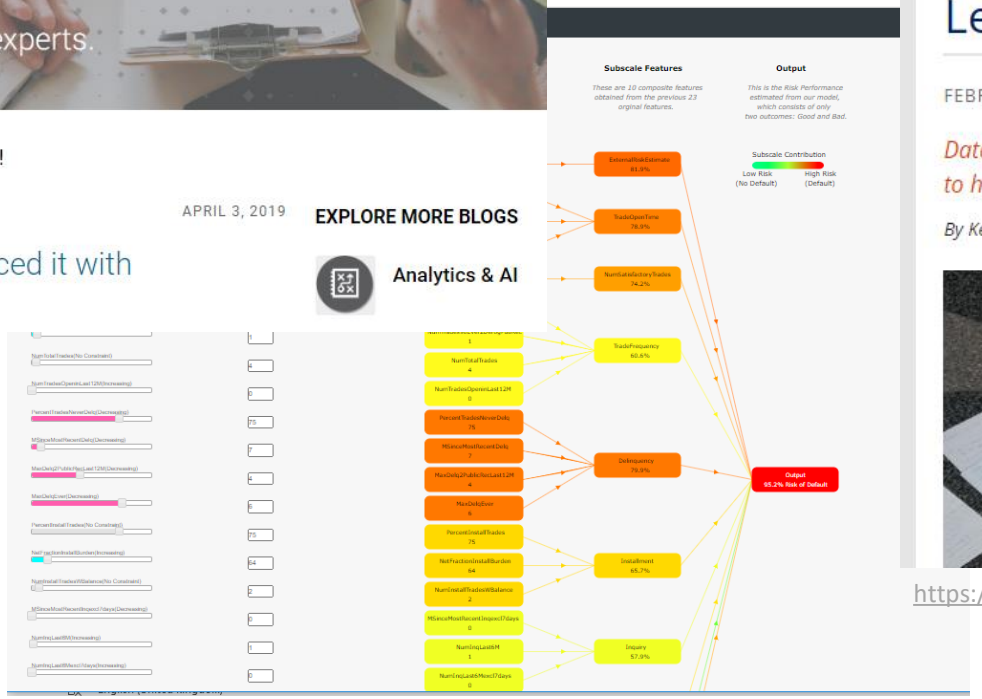
Explainability or Interpretability of AI system remains an open research problem

For the expert or for the user?

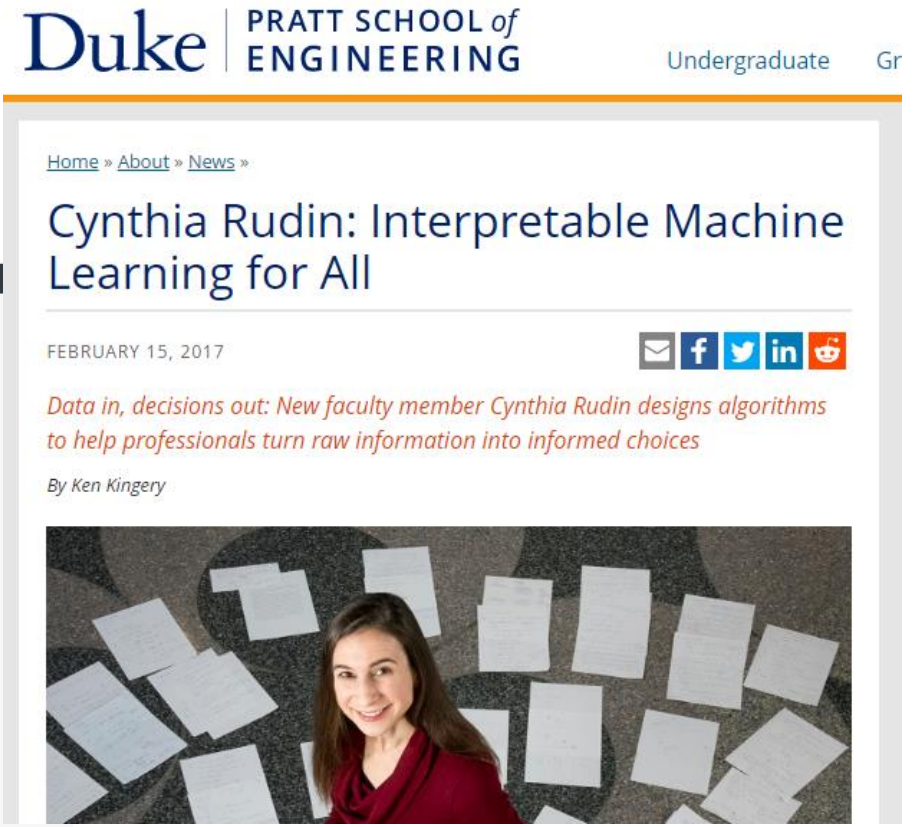
Build Interpretable Models instead of Explaining Black Boxes

https://community.fico.com/s/blog-post/a5Q2E0000001czyUAA/fico1670





http://dukedatasciencefico.cs.duke.edu/



https://pratt.duke.edu/about/news/cynthia-rudin

Practical AI Ethics Frameworks

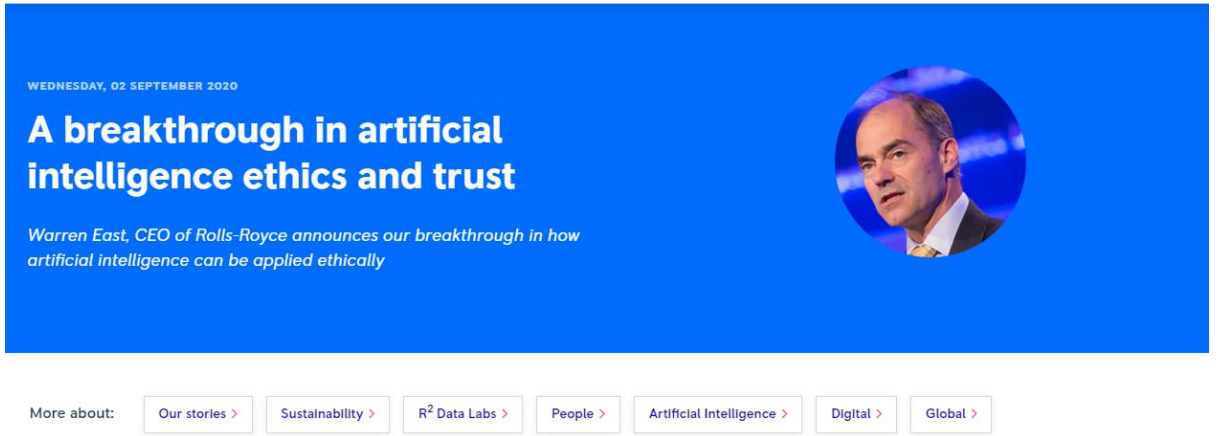
The Aletheia Framework™ A3 worksheet v1.0

PDF - 862KB

The Aletheia Framework™ booklet

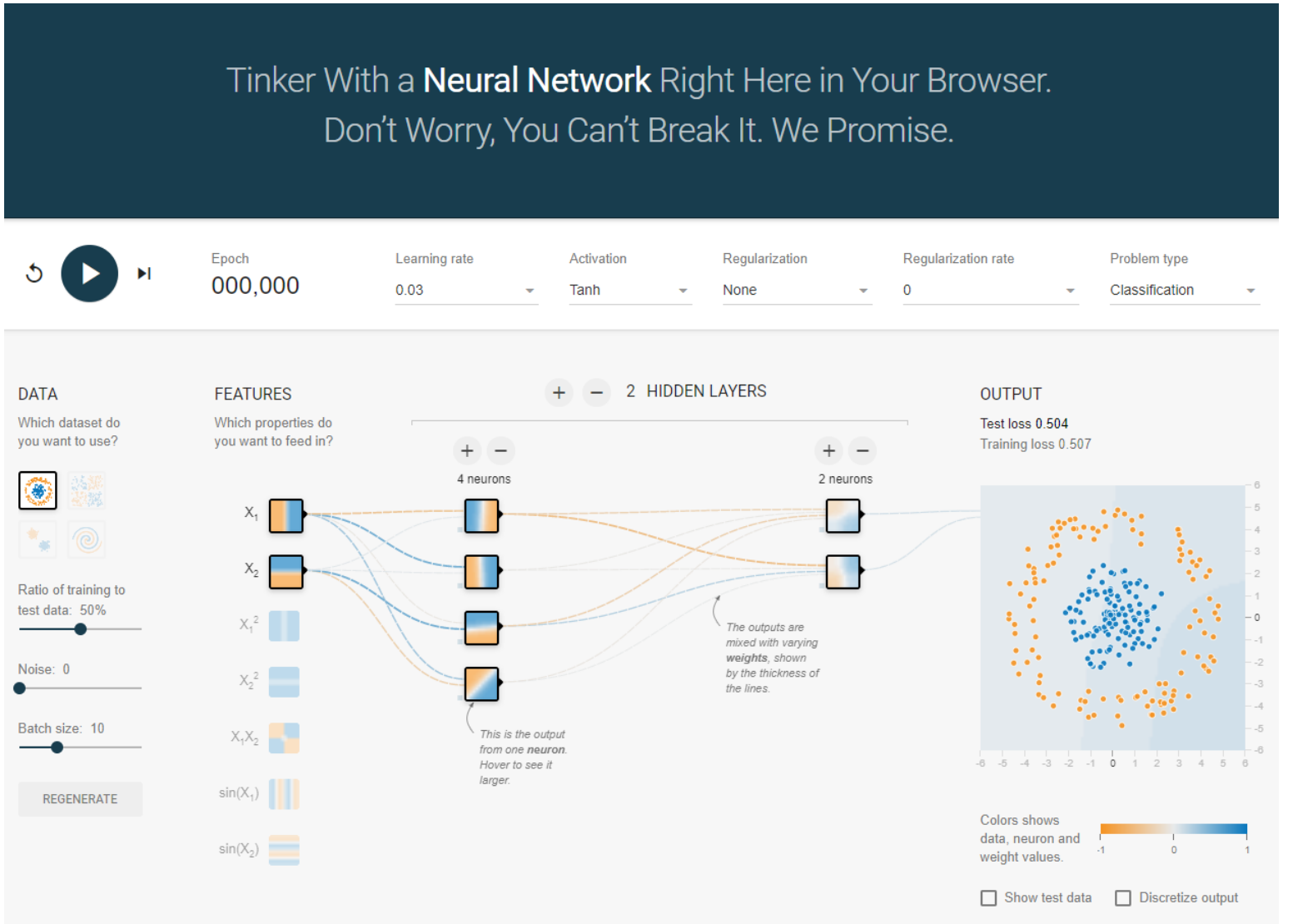
PDF - 1.7MB

https://www.rolls-royce.com/sustainability/ethics-and-compliance/the-aletheia-framework.aspx



https://www.rolls-royce.com/media/our-stories/insights/2020/tech-week-ai-summit.aspx

See how neural networks learn: https://playground.tensorflow.org/



Try out image recognition: https://teachablemachine.withgoogle.com/

Teachable Machine

Train a computer to recognize your own images, sounds, & poses.

A fast, easy way to create machine learning models for your sites, apps, and more – no expertise or coding required.

Get Started