No Rewind Button: Legal Pitfalls (and Potential Solutions) in Machine Learning Systems

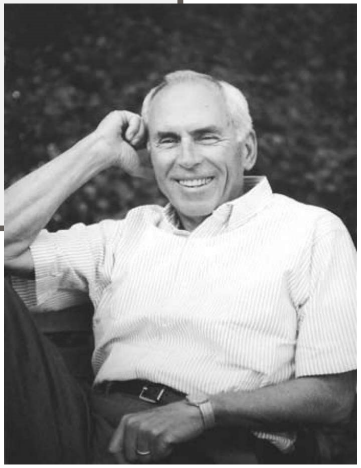
ROGER BODAMER
Founder/CTO/COO
Archipelago Analytics

STEVE CARLSON
Partner
Robins Kaplan LLP

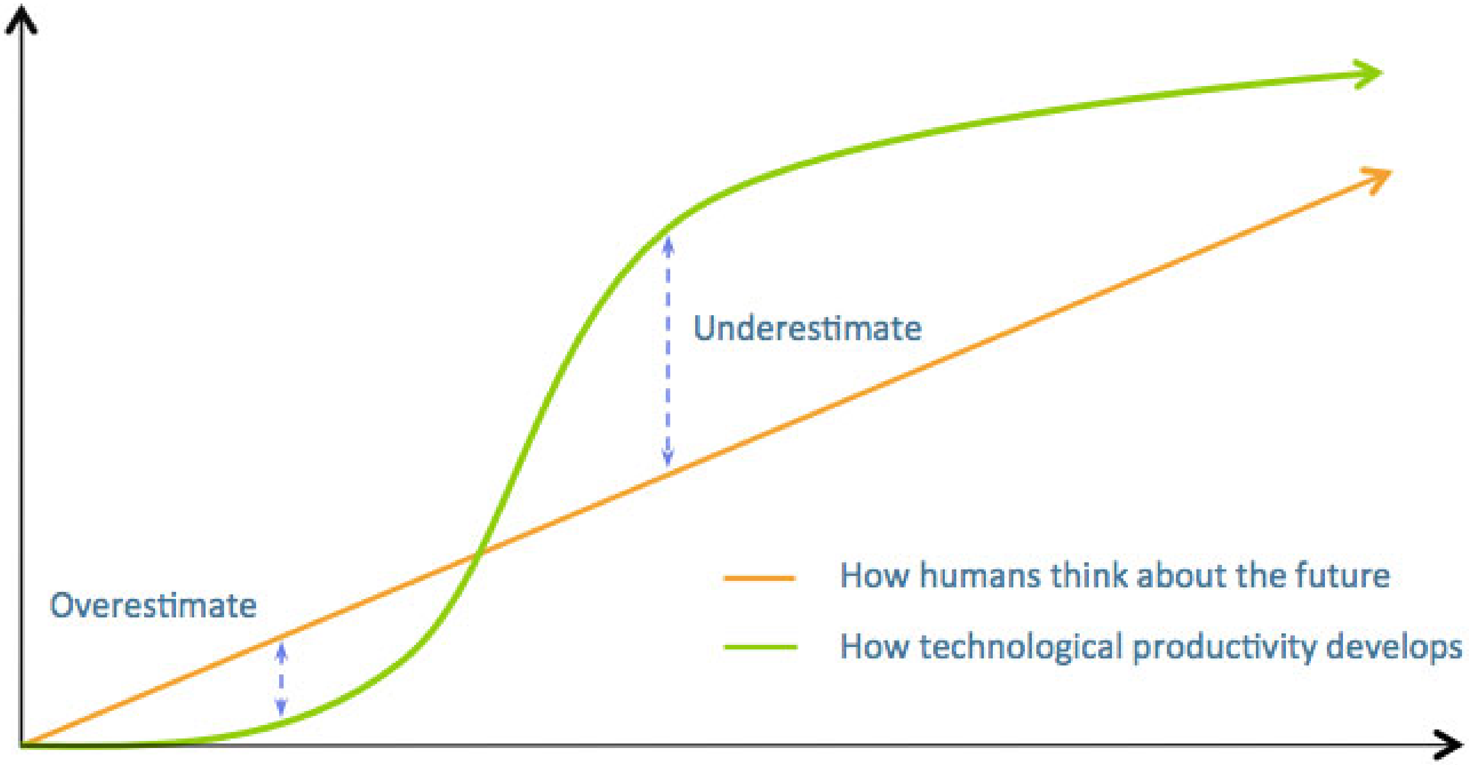
DR. MICHAEL MEEHAN
General Counsel
Diveplane

Berkeley Center for Law & Technology | ROBINS KAPLAN LLP
REWRITING THE ODDS

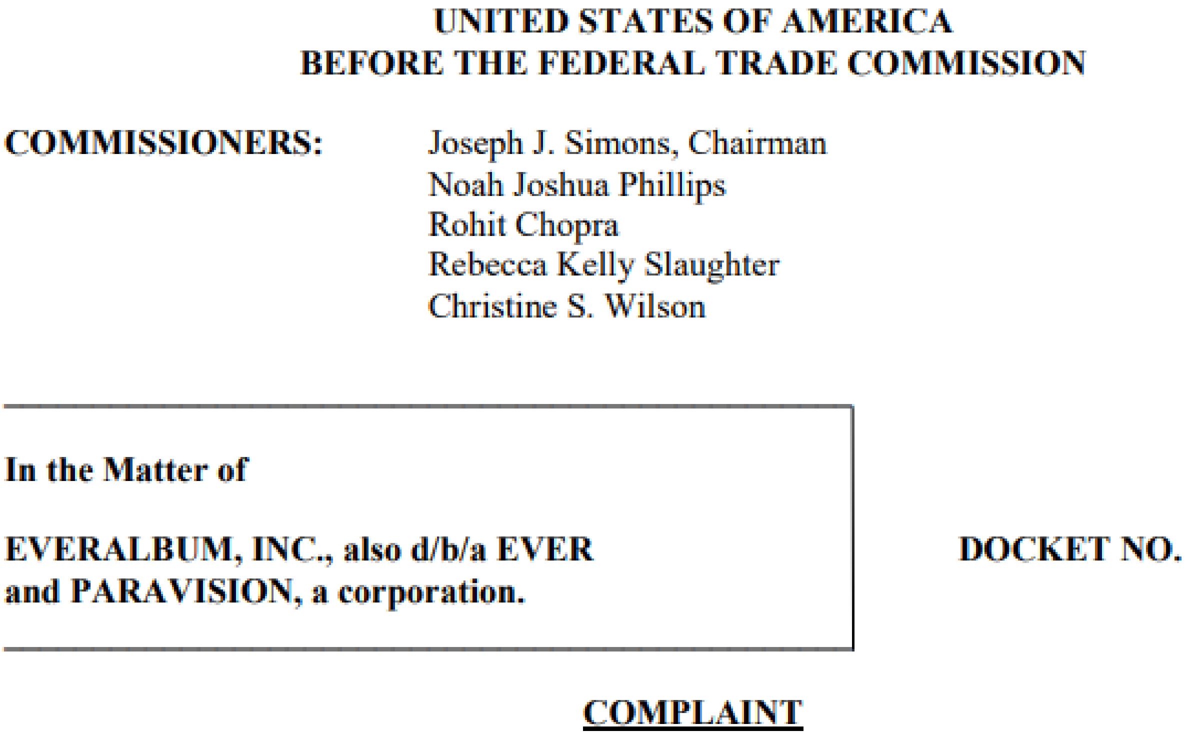
"We tend to **overestimate** the effect of a technology in the **short** run and **underestimate** the effect in the **long** run"



Roy Amara
1925-2007


Underestimate
Overestimate
How humans think about the future
How technological productivity develops

FTC Enforcement: Everalbum (2021)



UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS:

Joseph J. Simons, Chairman
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

In the Matter of

EVERALBUM, INC., also d/b/a EVER and PARAVISION, a corporation.

DOCKET NO.

COMPLAINT

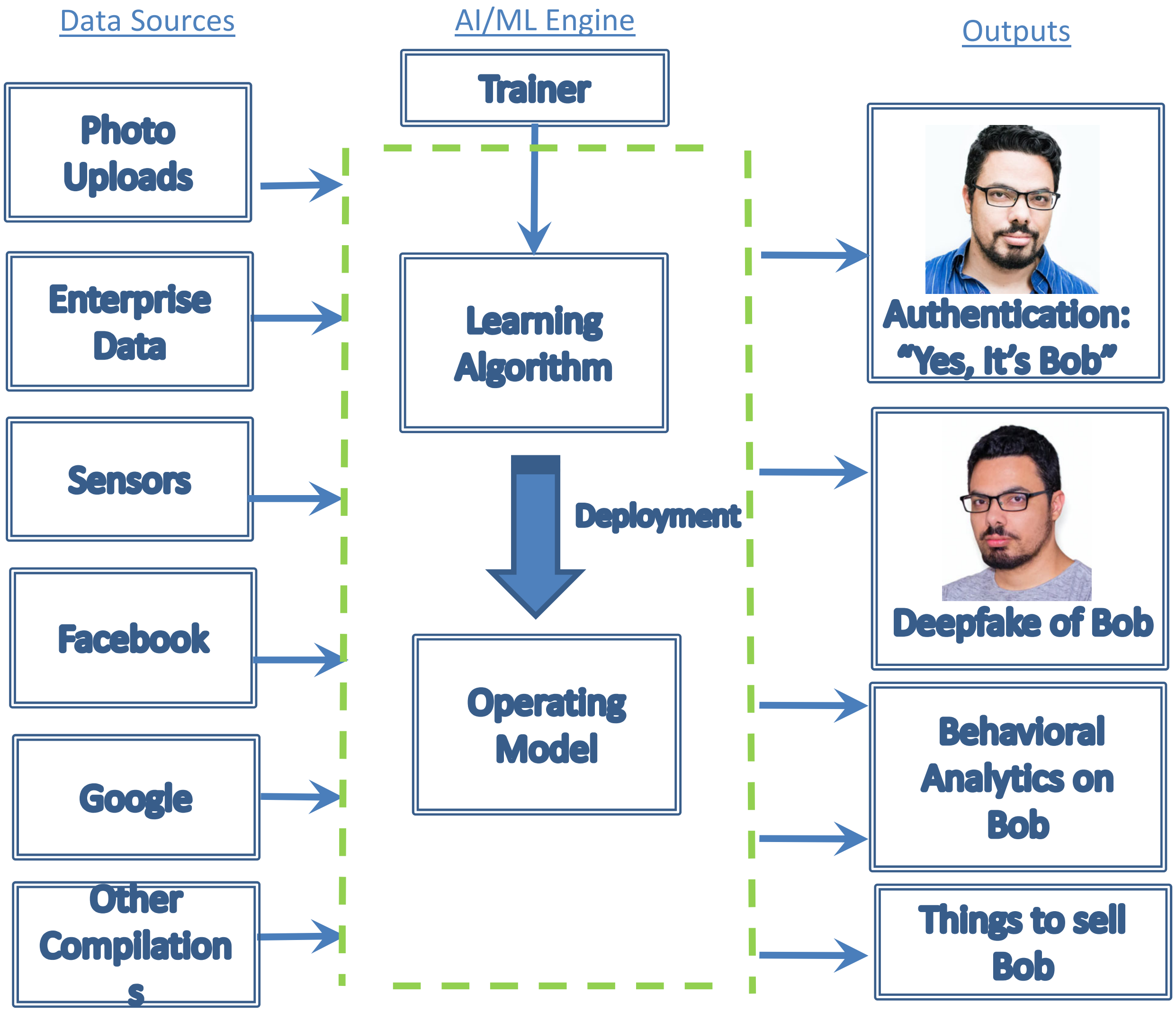
FTC Enforcement: Everalbum (2021)

- Everalbum operated photo storage app
- Performed facial recognition on customers, obtained consent in Texas, Washington, Illinois, EU, but not elsewhere
- Built machine learning model from collected data
- Provided machine learning model to related enterprise-level company, Paravision

FTC Enforcement: Everalbum (2021)

- Complaint: Unfair or Deceptive Acts (§5(a) FTCA)
- Alleged misrepresentation: misleading language on user control of facial recognition
- Resolution: Delete all “models and algorithms it developed in whole or in part using images from User’s photos.”

Machine Learning Models: Neural Networks and KNN Systems



Data Sources

AI/ML Engine

Outputs

Photo Uploads

Enterprise Data

Sensors

Facebook

Google

Other Compilations

Trainer

Learning Algorithm

Deployment

Operating Model

Authentication: “Yes, It’s Bob”

Deepfake of Bob

Behavioral Analytics on Bob

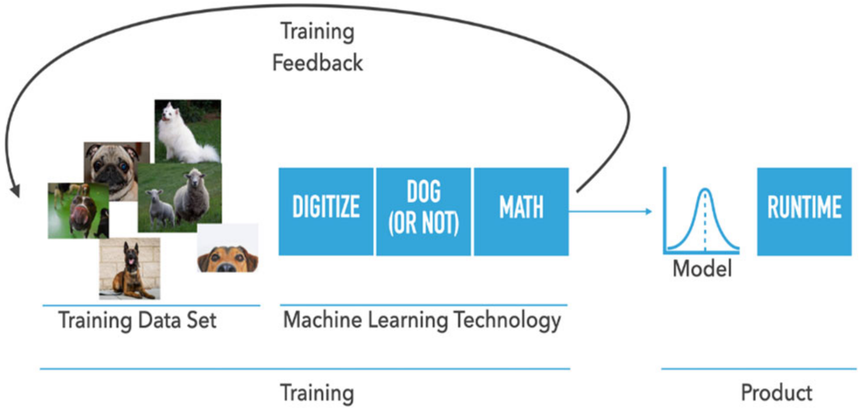
Things to sell Bob

Neural Network Machine Learning Models

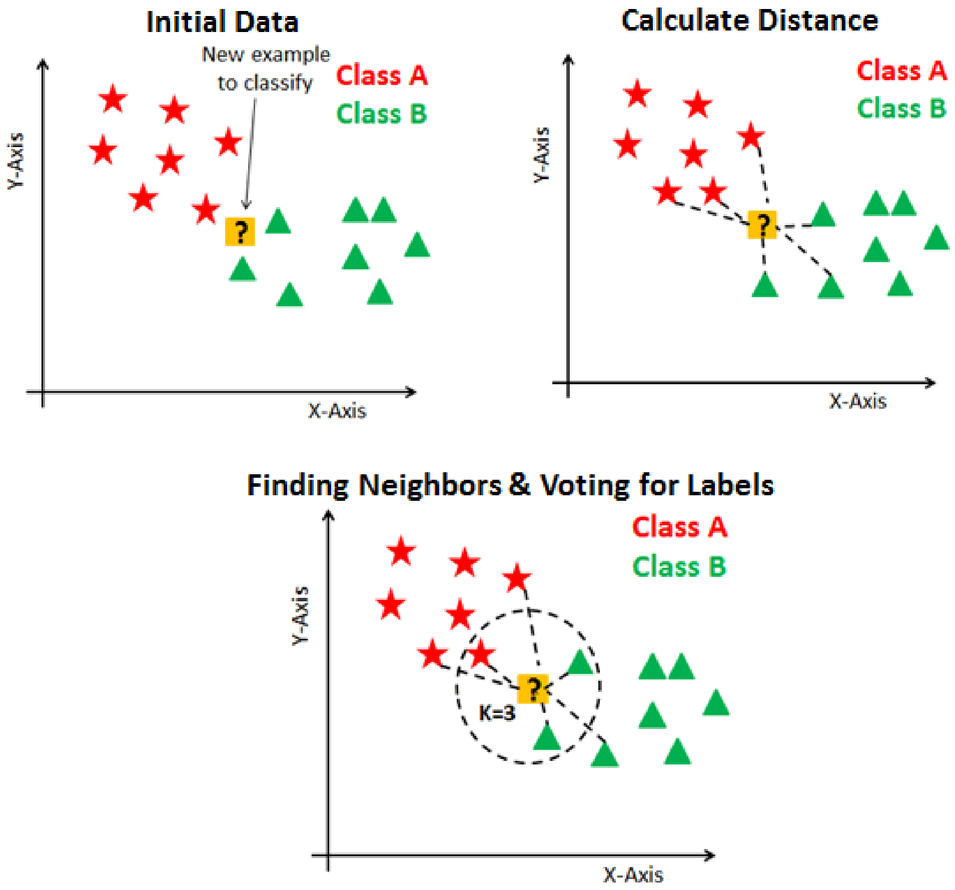
ML Models: Feedback system for training

Result: system that "knows" true/false

Continuous learning, no "rewind button"



K-NEAREST NEIGHBOR (KNN) SYSTEM



Initial Data

Calculate Distance

Finding Neighbors & Voting for Labels

- Explainability
- Editability
- Confidence in decision
- Computation increases with size of data set

Berkeley Center for Law & Technology | ROBINS KAPLAN LLP

REWRITING THE ODDS

Overview of Machine Learning

- Neural networks:
  - Create models that are independent of the size of the training data set
  - May be impossible to revert any specific data out of models
- Deployment considerations:
  - SAAS: All the computation happens in the cloud, which may give greater flexibility managing your data
  - SAAS: Many agreements needed for different jurisdictions
  - IoT: Poses different challenges to revert tainted data. Small devices may lack power to recompute, even if there is a solution for tainted data
- KNN:
  - KNN allows interpretability, editability, transparency
  - Large overlap between use cases for KNN and neural networks
  - Computation requirements may limit certain use cases for KNN

Everalbum: What if KNN system?

If Everalbum was running a KNN system:

- Everalbum could have offered to FTC to delete the specific data for which there was not adequate consent
- Everalbum may have been able to re-launch its service using limited data with proper consent
- Possibility to create “synthetic data” based on limited set of data for which consents acquired

Neural networks: no good framework for complying with order like FTC’s

Risk Scenarios: Removing Data from Models

- Evolving consent requirements – stream of new privacy laws
  - If your consents become obsolete, you may need to rewind (*Everalbum*)
- Breach of contractual use restrictions:
  - Use of data beyond limited authorization (*e.g.*, scraping)
- Other Privacy
  - Privacy shield abrogation; no safe harbor
- Trade secret exposure
  - Uptake of data via new employees (*WeRide*)
- Bias
  - If model trained on biased data, then expect biased results. May need to adjust training data to obtain more balanced view.
  - KNN: able to tell you the features that drive decision. May be possible to "rewind" bad data sets

Potential Solution: Synthetic Data

- GEMINAI (synthetic data tool)
  - Creation of new data sets based on limited data set
  - Potential to overcome consent restrictions
  - Scenario: HIPAA data, moving data between departments

Trade Secrets: Input Data Risks

Misappropriated data brought to autonomous vehicle competitor

> The Court ORDERS as follows:
>
> - A. Enjoined Defendants and all persons acting under, in concert with, or for any one of them, whether or not in the United States, are hereby restrained and enjoined from each and all of the following:
>
>   1. Any and all use, disclosure, providing third parties access to, transferring, copying , duplication, reproduction, publication, distribution, broadcasting or marketing of any version of WeRide Confidential Information.

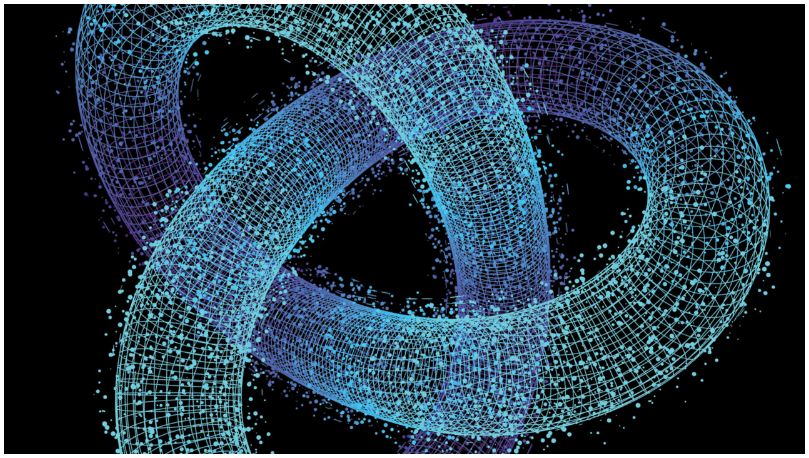
Weride Corp. v. Huang, 2019 WL 1439394 (N.D. Cal. 2019)

How comply?

Preventative Guidelines

- Architectural changes (*e.g.*, KNN) to allow editability
- Employee intake procedures
- License your data sets
- Preserve data lineage
- Keep versions of your training sets
- Track ephemeral data (if possible)
- Due diligence demands

Article: September 2020 ABA Landslide Magazine



No Rewind Button: Legal Pitfalls of Machine Learning Systems
Steven Carlson & Roger Bodamer

https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2020-21/september-october/no-rewind-button-legal-pitfalls-machine-learning-systems-webinar/

Questions?
Thank you!

Berkeley Center for Law & Technology | ROBINS KAPLAN LLP

REWRITING THE ODDS