PRIVACY IN THE AGE OF AI:

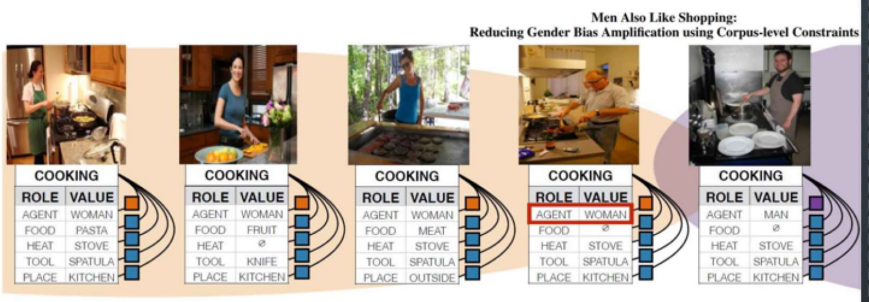
WHY YOU SHOULD THROW YOUR PHONE AWAY AND BECOME A HUNTER-GATHERER

HASHEM BENAMAR

Example systems

- Smart personal assistants
- Ridesharing apps (wait time prediction, surge pricing)
- Smart email categorization
- Plagiarism detection
- At-risk individual identification
- Mobile check deposit
- Fraud detection (credit card transactions)
- Recommender systems

Machine Learning can amplify bias.



- Data set: 67% of people cooking are women
- Algorithm predicts: 84% of people cooking are women

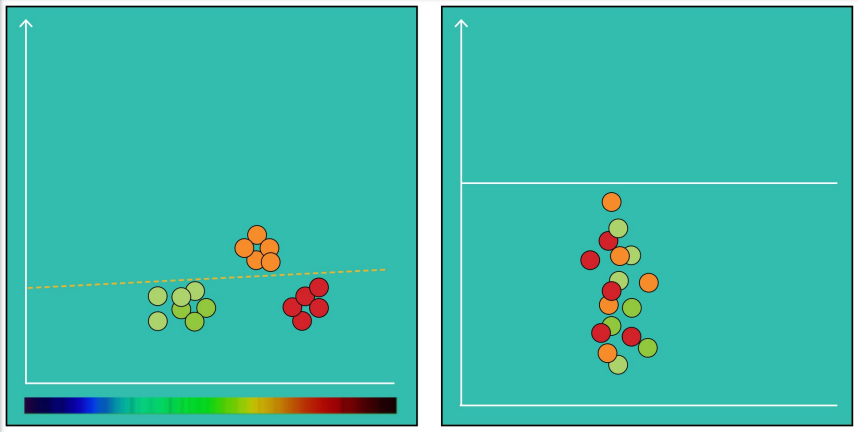


Figure 3.

Dividing apples and oranges and others based on the feature of color results in a meaningful output.[19]

Dividing apples and oranges based on the feature of size makes distinguishing them much harder.[20]

HOW DID WE GET HERE?

- THE RISE OF BIG DATA
- DIFFICULTIES:
  - PERSONAL IDENTIFICATION
  - USER LITERACY
  - DISCRIMINATION
  - EXPLAINABILITY
- MITIGATION
  - DATA MINIMIZATION

Fairness and "Bias" Concerns

Supervised learning requires massive amounts of training data. Bias that is present in the training data becomes inherent in the model it produces.

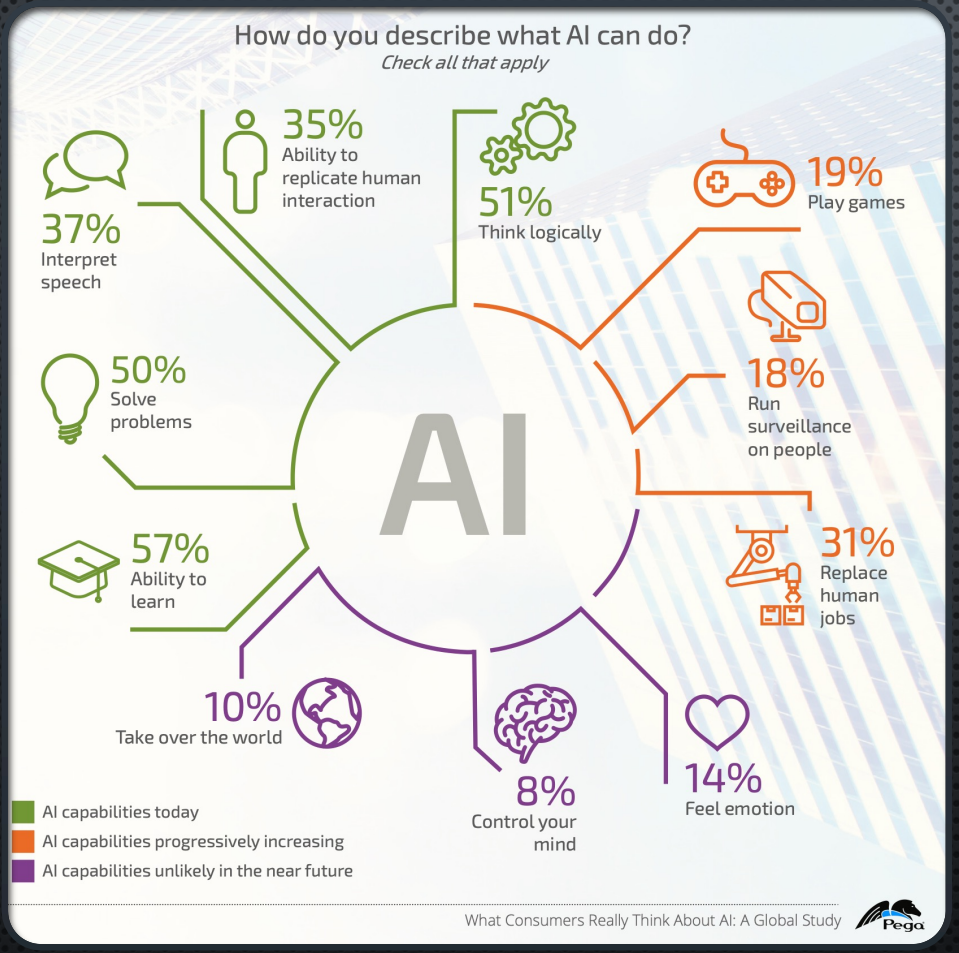
Example 1: Researchers recently used a deep learning technique to train a system to distinguish pictures of huskies from pictures of wolves. When these techniques were applied, each time the AI identified the picture as a wolf, the scientists discovered that it was paying attention to the presence or absence of snow in the image. The systems "learned" that one factor in whether it was a wolf was the presence of snow. Thus, the system relied on a false correlation, deciding that every time there was snow, it was a wolf. In a supervised learning application (with labeled images), this result might be the result of a biased dataset that included few or no pictures of wolves in grass, or dogs in snow.[38]

(a) Husky classified as wolf (b) Explanation

Figure 11: Raw data and explanation of a bad model's prediction in the "Husky vs Wolf" task.

	Before	After
Trusted the bad model	10 out of 27	3 out of 27
Snow as a potential feature	12 out of 27	25 out of 27

Table 2: "Husky vs Wolf" experiment results.



USER PERSPECTIVE

USER PERSPECTIVE

- DEMONIZATION OR GLORIFICATION OF LARGE COMPANIES
- INDUSTRY WIDE CHANGE
- TRUST AND TRANSPARENCY
- USER DESIRE TRADEOFF
- IS ANYONE EQUIPPED TO MAKE AN INFORMED DECISION?

BIOMETRIC PROFILING

- THINK: MEDICAL MONITORING
- WHAT KIND OF HUMAN SUBJECT IS BEING CONSTRUCTED BY THESE TECHNOLOGICAL SYSTEMS AND PRACTICES?

Forbes

Feb 16, 2012, 11:02am EST

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Former Staff
Tech
Welcome to The Not-So Private Parts where technology & privacy collide

Follow

This article is more than 9 years old.

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target , for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant -- and loyal -- buyers of all things pastel, plastic, and miniature. He talked to Target statistician Andrew Pole -- before Target freaked out and cut off all

The New York Times

One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority

In a major ethical leap for the tech world, Chinese start-ups have built algorithms that the government uses to track members of a largely Muslim minority group.

DESIGN AND… THE LAW?

- "Data shall be used only for the purpose for which they were collected. And the collateral: If no purpose was defined prior to the collection of data, then the data should not be used." van lei
- Philosophical arguments for ecological considerations
- Machine readable behavior of 'computable entities' can be weaponized (Cambridge analytica x facebook leak)
- Do you think that a decision significantly affecting a person cannot just be based on a fully automated assessment of his or her personal characteristics.

FROM AGNOSTIC TO AGONISTIC

- We don't need "your" data to learn about you, everyone else will suffice.
- At first, architecture choice is made based on data inferences
- If it is not personal, does it affect you?
- Agonistic machine learning: process by which design process "*will contribute to responsible decisions about the integration of data-driven applications into our environments while simultaneously bringing them under the Rule of Law*

STANDARDIZATION

- HIPAA: Health Insurance Portability and Accountability Act
- CCPA: California Consumer Privacy Act
- GDPR: General Data Protection Regulation

CCPA

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.
  - Personal information: personal data that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household; notably including **"inferences drawn"** from any other personal information to create a profile of the consumer.
  - What is this definition missing?

STANDARDIZATION ISSUES

AGGREGATE CONSUMER INFORMATION: DATA THAT RELATES TO A GROUP OR CATEGORY OF CONSUMERS, FROM WHICH INDIVIDUAL CONSUMER IDENTITIES HAVE BEEN REMOVED, THAT IS NOT LINKED OR REASONABLY LINKABLE TO ANY CONSUMER OR HOUSEHOLD, INCLUDING VIA A DEVICE.

- AMBIGUITY:
  - "INFERENCES DRAWN"
  - "PUBLICLY AVAILABLE INFORMATION"

STANDARDIZATION ISSUES

- ABSENCES:
  - WORKERS AS A POPULATION GROUP
  - CREDIT RATING
  - MEDICAL HISTORY
  - PRIVATE RIGHT OF ACTION.

STANDARDIZATION ISSUES

- EXEMPTIONS:
  - CLAUSE: EXEMPT IF INFORMATION IS NECESSARY FOR A NUMBER OF FUNCTIONS AND INTERNAL USES REASONABLY ALIGNED WITH THE EXPECTATIONS OF THE CONSUMER
  - WEAKNESS: WHAT DOES THIS EVEN MEAN? HOW CAN WE DEFINE THIS?
  - CLAUSE: BUSINESSES MAY *NOT* CHARGE A CONSUMER A DIFFERENT PRICE OR RATE OR PROVIDE A DIFFERENT LEVEL OR QUALITY OF GOODS OR SERVICES TO THE CONSUMER
  - WEAKNESS: THEY CAN DO EXACTLY THAT SO LONG AS THESE DECISIONS ARE REASONABLY RELATED TO THE VALUE PROVIDED TO THE BUSINESS BY THE CONSUMER'S DATA.
  - CLAUSE: OPT-OUT MODEL
  - WEAKNESS: SHIFTS THE BURDEN ONTO CONSUMER
  - CLAUSE: BUSINESSES MAY NOT USE TARGETED DISCOUNTS OR OTHER BENEFITS
  - WEAKNESS: THEY MAY OFFER "FINANCIAL INCENTIVES" INCLUDING COMPENSATION, TO CONSUMERS FOR THEIR DATA.

  THESE ARE ECONOMICALLY INDISTINGUISHABLE AND LEGALLY UNCLEAR.

WHAT TO MAKE OF THIS?

- THE LEGAL SYSTEM IS A MESS AND OUR DEEPLY CORRUPT SOCIETY SHOULD NOT HAVE ACCESS TO SOMETHING AS POTENTIALLY PROFITABLE AS AI AND MACHINE LEARNING

- THE IMPORTANCE OF GOAL AND DESIGN SPECIFICATION IN THE DEVELOPMENT PROCESS
- THE IMPORTANCE OF CLEAR DEFINITION OF REGULATION AND ITS APPLICABLE CASES
- THE IMPORTANCE OF INTRANSIGENT APPLICATION OF THE LAW ON OFFENDERS
- USER LITERACY AND TRANSPARENCY OF INTELLIGENT SYSTEMS
- WHEN IN DOUBT, BLAME A SYSTEM DESIGNER