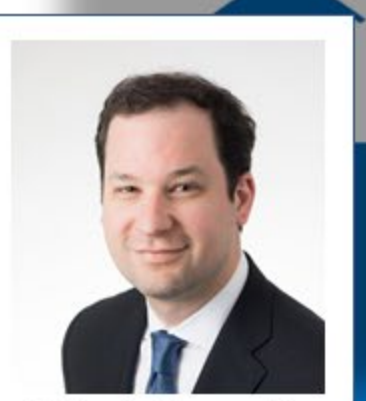
New York Metro Joint Cyber Security Conference & Workshop

October 22-23, 2020

InfoSecurity.NYC



Mark Francis

Understanding AI's Risks and Rewards

AI as a force for good

"The science company [] has begun a program designed to make artificial intelligence systems better at detecting lung cancer warning signs … by assessing medical images. "

"[A] British drug discovery company [] has produced the first precision engineered drug produced with the aid of artificial intelligence. The medicine is now set to commence clinical trials."

"A research team have put in place an artificial intelligence system to detect low glucose levels via an electrocardiogram readout … [t]his [] obviates the need for a blood test [and] is effective for the detection of diabetes."

Current Health, Mayo Clinic launch AI-based COVID-19 detection collaboration

AI as a force for good

Forbes

15,600 views | Feb 10, 2020, 12:19am EST

8 Powerful Examples Of AI For Good

Bernard Marr Contributor

Enterprise Tech

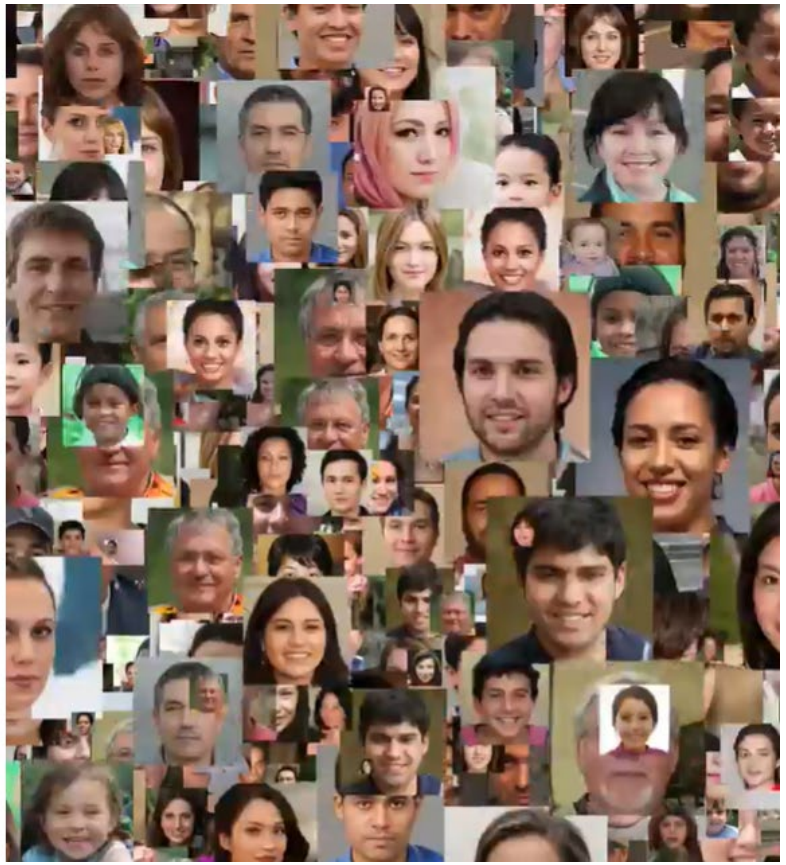
- Accessibility
- Climate Change, Conservation and the Environment
- World Hunger
- Human Rights
- Fight Fake News
- Education
- Healthcare
- Resilience

AI as a force for bad

The New York Times

The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and "might lead to a dystopian future or something," a backer says.



"Clearview AI, devised a groundbreaking facial recognition app … [its] backbone is a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo and millions of other websites…

… [it] could end your ability to walk down the street anonymously…

…more than 600 law enforcement agencies have started using Clearview in the past year… "

… it gets worse…

THE VERGE

Clearview AI's source code and app data exposed in cybersecurity lapse

Company claims only law enforcement agencies have access to its software

By Jon Porter | @JonPorty | Apr 17, 2020, 5:31am EDT

… and now the lawsuits…

DigitalNewsDaily

Lawsuit Seeks Injunction Requiring Clearview To Destroy Data

by **Wendy Davis** **@wendyndavis**, April 8, 2020

March 12, 2020

Clearview AI class-action may further test CCPA's private right of action

On February 27, 2020, a California resident and an Illinois resident filed a punitive class-action against Clearview AI in the United States District Court for the Southern District of California. The complaint alleges that Clearview AI unlawfully "scraped" biometric data – mostly images of individuals – from social media and other websites, and applied facial-recognition software to create databases for sale to law enforcement and the private sector. In doing so, plaintiffs allege Clearview AI violated the policies of the websites from which the images were "scraped," and also violated the California Consumer Privacy Act (CCPA) and the Illinois Biometric Privacy Act (BIPA).

POLICY BLOG

COMMENTARY

Clearview AI Hit With Biometric Privacy Lawsuit

by **Wendy Davis** , Staff Writer **@wendyndavis**, January 23, 2020

Clearview AI, a start-up that reportedly sells "faceprint" databases to police departments, has been hit with a potential class-action lawsuit.

… and investigations

OFFICE OF THE VERMONT ATTORNEY GENERAL
TJ Donovan, Vermont Attorney General

Attorney General Donovan Sues Clearview AI for Violations of Consumer Protection Act and Data Broker Law

MARCH 10, 2020

Contact: Charity R. Clark, Chief of Staff, 802-828-3171

Attorney General Donovan filed a lawsuit today against Clearview AI, a data broker that uses facial recognition technology to map the faces of Vermonters, including children, and sells access to this data to private businesses, individuals, and law enforcement. The complaint, filed in Chittenden Superior Court – Civil Division, alleges violations of the Vermont Consumer Protection Act and the new Data Broker Law. Along with the complaint, the State filed a motion for preliminary injunction, asking the Court to order Clearview AI to immediately stop collecting or storing Vermonters' photos and facial recognition data.

The New York Times

New Jersey Bars Police From Using Clearview Facial Recognition App

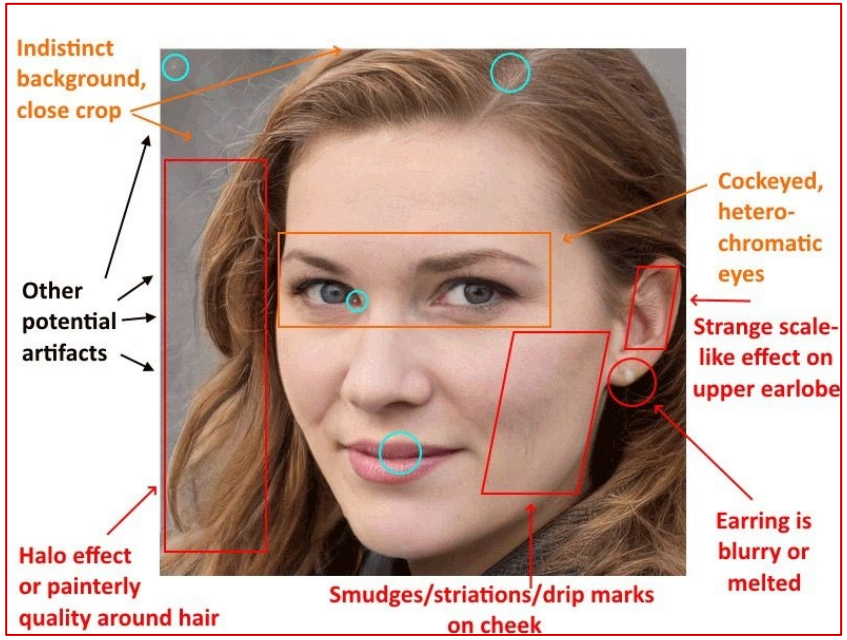
Reporting about the powerful tool with a database of three billion photos "troubled" the state's attorney general, who asked for an inquiry into its use.

Leveraging AI for social engineering

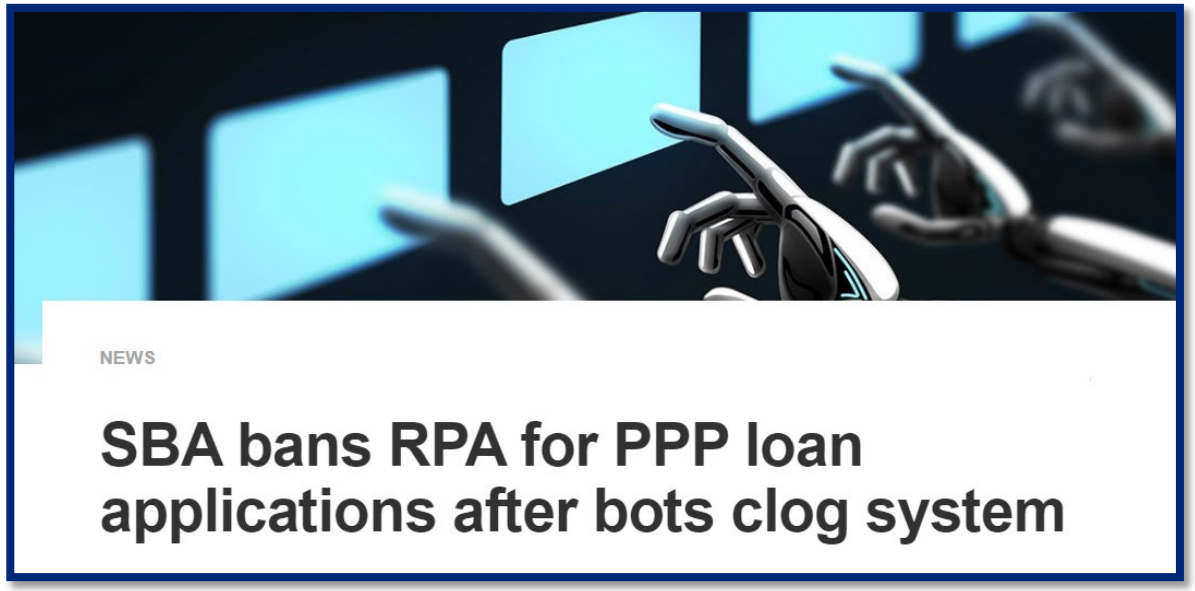
Experts: Spy used AI-generated face to connect with targets

By RAPHAEL SATTER June 13, 2019

"…She was connected to a deputy assistant secretary of state, a senior aide to a senator and the economist [ ], who is being considered for a seat on the Federal Reserve…"



AI under the microscope



- On April 28, the Department of the Treasury and the Small Business Administration said they will no longer accept Paycheck Protection program loan applications prepared by robotic process automation (RPA) systems.
- SBA noted that the use of robotic process automation burdens the E-Tran system.

*"Without RPAs, the loan processing system will be more **reliable, accessible,** and **equitable** for all small businesses"*

AI under the microscope

05.22.19

Here's AOC calling out the vicious circle of white men building biased face AI

Press Releases

House Intelligence Committee To Hold Open Hearing on Deepfakes and AI

The National Security Challenge of Artificial Intelligence, Manipulated Media, and "Deepfakes"

Washington, June 7, 2019

Washington, DC – On Thursday, June 13, 2019 at 9:00 am, the House Permanent Select Committee on Intelligence will conver challenges of artificial intelligence (AI), manipulated media, and "deepfake" technology. This is the first House hearing devoted types of AI-generated synthetic data.

THE WALL STREET JOURNAL.

U.S. Edition ▾ | September 25, 2019 | Print Edition | Video

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazin

CIO JOURNAL

CIOs See End of 'AI Gone Wild' in Congressional Hearings

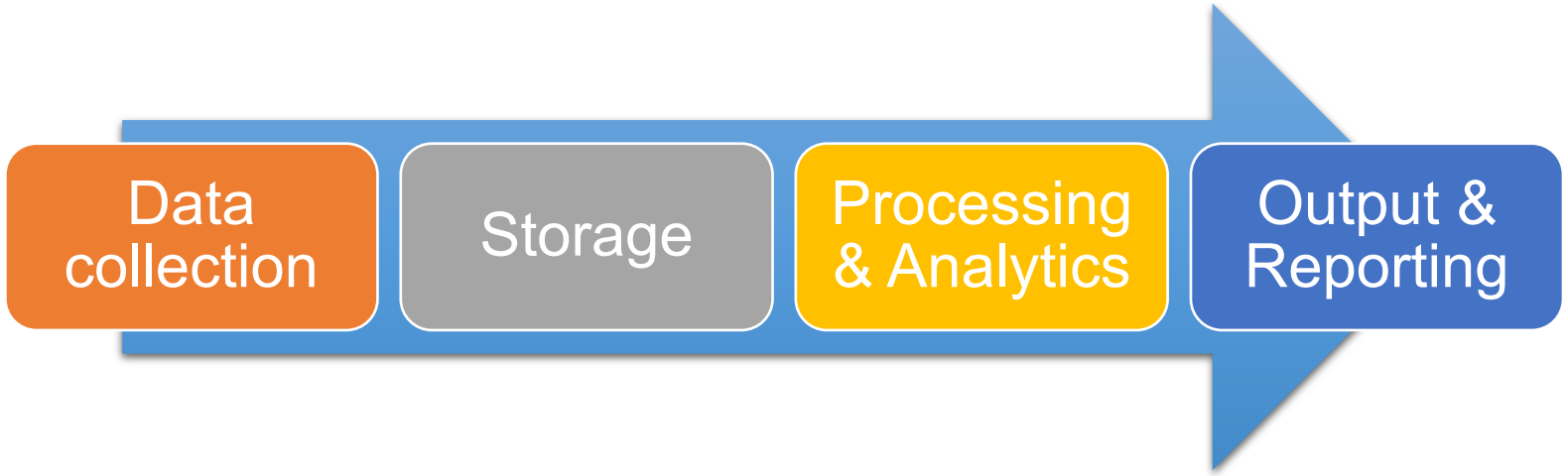
Regulation is expected eventually, but experts say it should be crafted in a way that avoids hampering innovation

Facebook's Monika Bickert, Twitter's Nick Pickles and Google's Derek Slater at Wednesday's hearing before the House Homeland Security Committee. PHOTO: WIN MCNAMEE/GETTY IMAGES

How AI works

How AI works

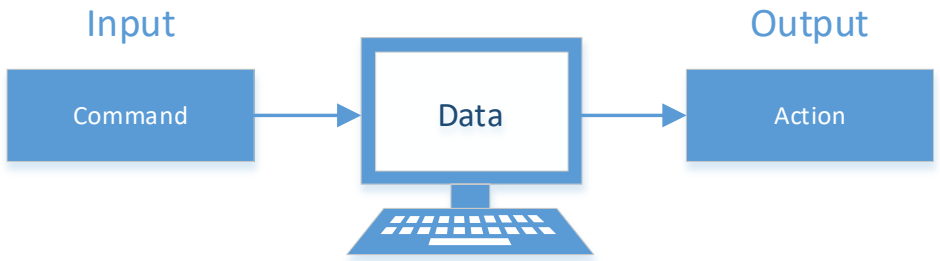
- AI as we are currently using it represents the next generation of big data analytics



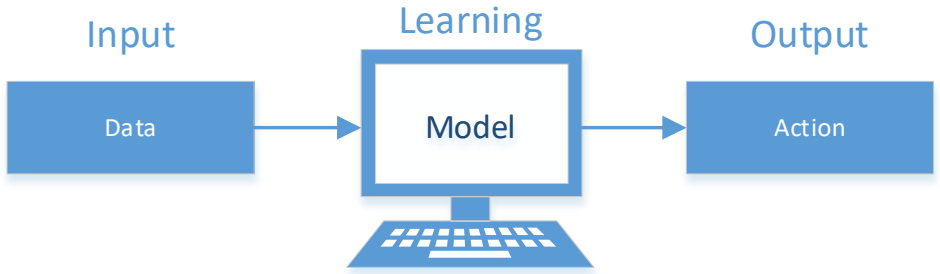
- Big data analytics relies on two key components:
  - Accumulation of big data sets
    +
  - Availability of cheap computing power

How AI works

- How does AI change the approach?
  - Switch from ***command***-driven analytics…
    - Need to know desired output
    - Need to write commands for desired output



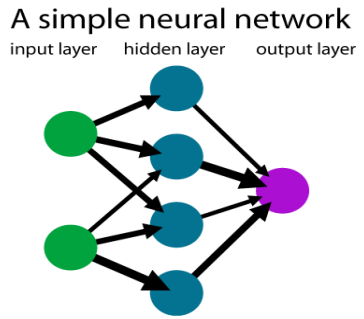
  - …to ***model***-driven analytics
    - Machine determines the output
    - Machine develops model to achieve that output



Advanced AI/ML

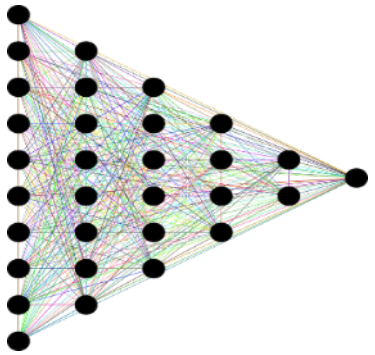
Artificial "Neural Networks"

- Interconnected "neurons" perform discrete data-related tasks, such as recognizing something or creating associations between information



"Deep Learning"

- Multiple layers of neural networks can perform more complex tasks and learn from mistakes over time in order to produce results with increasing accuracy and precision



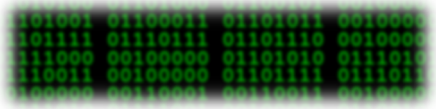
Implementing an AI/ML model

1. "**Scrub**" the data
2. Break the data into "***training***" and "***test***" portions (such as a 70/30 split)
3. Select suitable "***algorithms***" (e.g., statistical formulas)
4. Configure the algorithm "***hyperparameters***" to reduce errors
5. Train a "***decision model***" that accurately predicts results

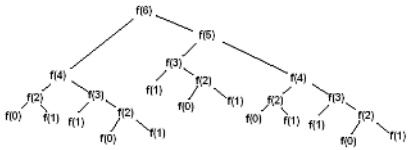
Putting it all together

Data feed
(Training dataset)

Transformed data
(Scrubbed data)



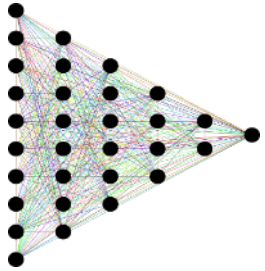
Untrained Model
(Algorithms)



Development

SaaS / AI Engine

Trained model

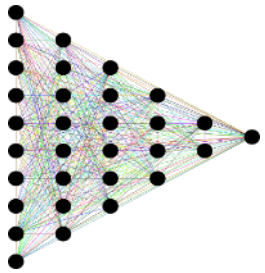


Derived Data
(Output)

Deployment

Training

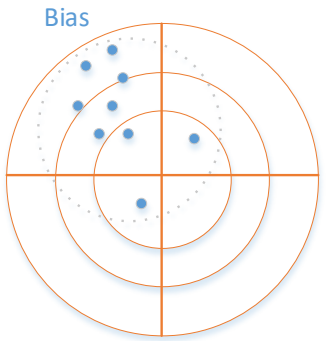
Trained model



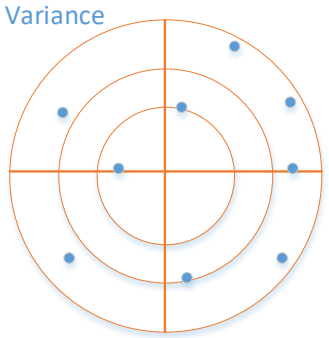
Dev Environment

Understanding AI challenges

Technical Bias refers to a gap between a predicted value and actual value—such as where errors tend to skew in a certain direction



Variance refers to how concentrated or scattered the predicted values are



Legal Bias refers to a decision that discriminates based on association with a legally-protected class (race, religion, gender, age, sexual preference)

AI using data associated with a protected-class can easily produce outcomes that are:

- **Mathematically right**
- **But legally wrong**

Increasing reliance on AI

- AI is changing computing in increasingly material ways

Experiments and games

IBM's Deep Blue famously beat Garry Kasparov at chess, becoming the first computer to defeat a human world champion

Personal Assistants

Hi, Siri… Google uses deep learning for voice and image recognition

Replacing Human Work Functions

E.g., approve or deny credit applications, detect fraud, identify prospective customers, manage financial risk

Life and Death Decision-Making

Autonomous vehicles; diagnose diseases based on symptoms, lab results and medical imaging

AI Laws

Current Legal Framework

Law governing evolving AI technology is unsettled

- No clear legal standard across all AI
- Over 40 bills that address AI have been introduced in Congress (more at state level)
- Legislators and regulators reluctant to act fast: don't want to stymie use or development of AI
- Opted for principals, guidance, statements
- Most experts believe the laws already in place for human activity that AI replaces can equally apply to developing technologies

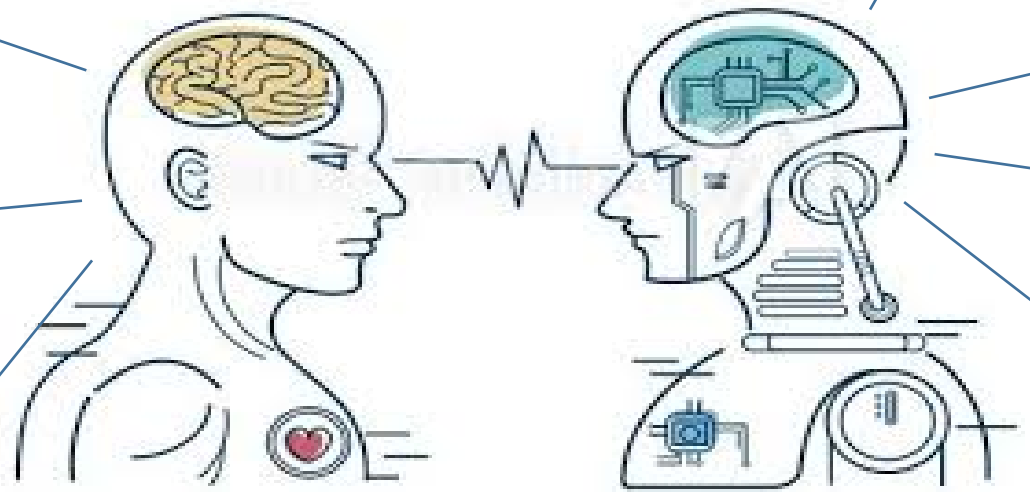
Liability challenge – Man v. Machine

Inputs known, controlled for, and can be disclosed

Numerous autonomous inputs, control is spread out

Duty of care built on known standards

Evolving duty of care for humans related to AI



Build on concepts of agency, control, and foreseeability

Unforeseeable injury or damages

Focused on human operation and conduct

Machine is actor or “decision maker”

Liability challenge – who is at fault?

If an algorithm or machine makes a "decision" that causes harm, who is liable? The law looks to persons *behind* the scene.

AI Designer / Developer

- AI designed to be completely in control?
- Harm caused by defect attributable to design of product?
- Is product unreasonably dangerous?

AI Manufacturer / Seller

- AI designed according to specifications?
- Clear instructions provided related to product operation?
- Harm foreseeable?

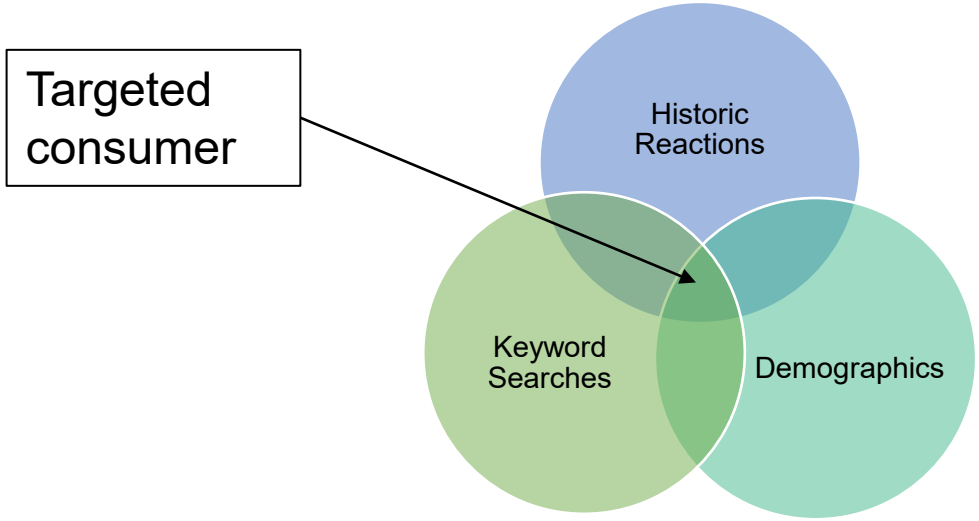
AI Purchaser / User

- User control the product, assisted by AI?
- Product being used as intended?
- Harm caused based on user error?

Case Study: matched by design

Key Facts:

- Social media platform utilizes AI that allows advertisers to micro-target the network's users based on interests, city, age, and other demographic information.
- Advertisers may also exclude people who were classified as "non-American-born," "non-Christian" or "interested in Hispanic culture," as well as those "based on ZIP code."

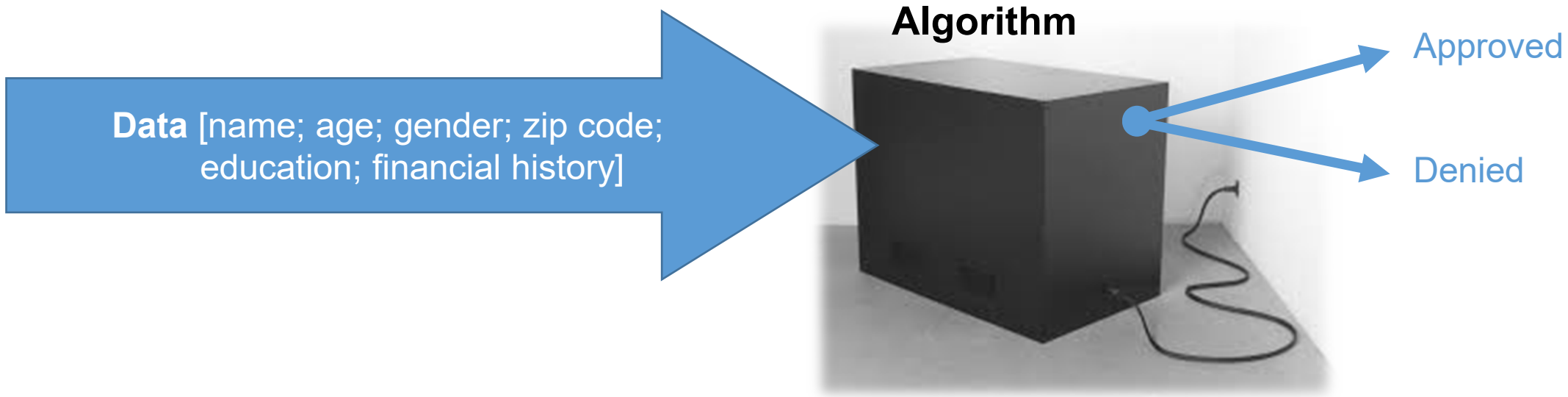


Scenario 1: Advertiser selling children's books ads were only shown to people who AI identified as being parents under the age of 40, searching child related retail sites, and interested in books.

Scenario 2: Advertiser selling rental property in exclusive area ads were only shown to people who AI identified as looking for new homes, interested in business, and living in certain zip codes. Ads not shown to people in other zip codes.

Case Study: risk of legal bias

- "Digital Redlining" – disparate impact based on decision making that is biased (creates or perpetuates inequality)
  - *E.g., HUD Charges Social Media and Technology Company, Facebook, With Housing Discrimination Over Company's Targeted Advertising Practices (March 28, 2019).*



Case Study: Face Facts

Key Facts:

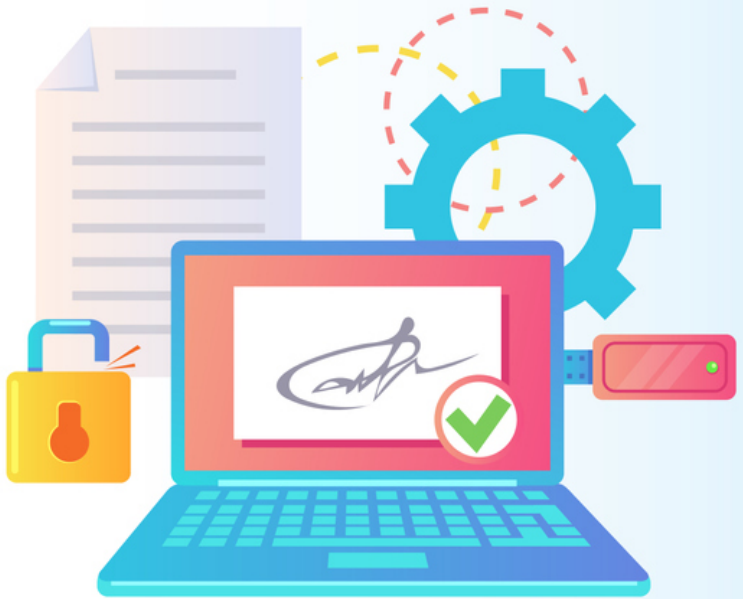
- Designer developed app that uses facial recognition technology to map the faces of people.
- Licenses access to this information to law enforcement, individuals, and private businesses.
- End user uploads photo, and AI scans millions of photos screen scrapped from various social media platforms.

Scenario 1: Police use AI technology to identify the man on a surveillance camera they suspect of wrongdoing, it identifies the man, police arrest him, turns out the AI was wrong.

Scenario 2: Employer uses technology as an added screening measure in hiring process, it returns several comprising photos that causes the employer not to hire the person.

photo courtesy of http://www.nydailynews.com/opinion/ny-edit-face-facts-20190520-svpau43vyrgvpkembegbtnimgq-story.html

Developing AI standards



Developments in the US

NIST - Plan for AI Standards (July 2019)

A PLAN FOR FEDERAL ENGAGEMENT IN AI STANDARDS -DRAFT FOR PUBLIC REVIEW 2-JUL-2019

U.S. LEADERSHIP IN AI:
A PLAN FOR FEDERAL ENGAGEMENT IN
DEVELOPING TECHNICAL STANDARDS
AND RELATED TOOLS

DRAFT FOR PUBLIC COMMENT

PREPARED IN RESPONSE TO EXECUTIVE ORDER 13859
SUBMITTED ON AUGUST XX, 2019

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Page 1 of 36

NIST - Exploring AI Trustworthiness (Aug. 2019)

NIST - Four Principles of Explainable AI (Draft, Aug 2020)

Draft NISTIR 8312

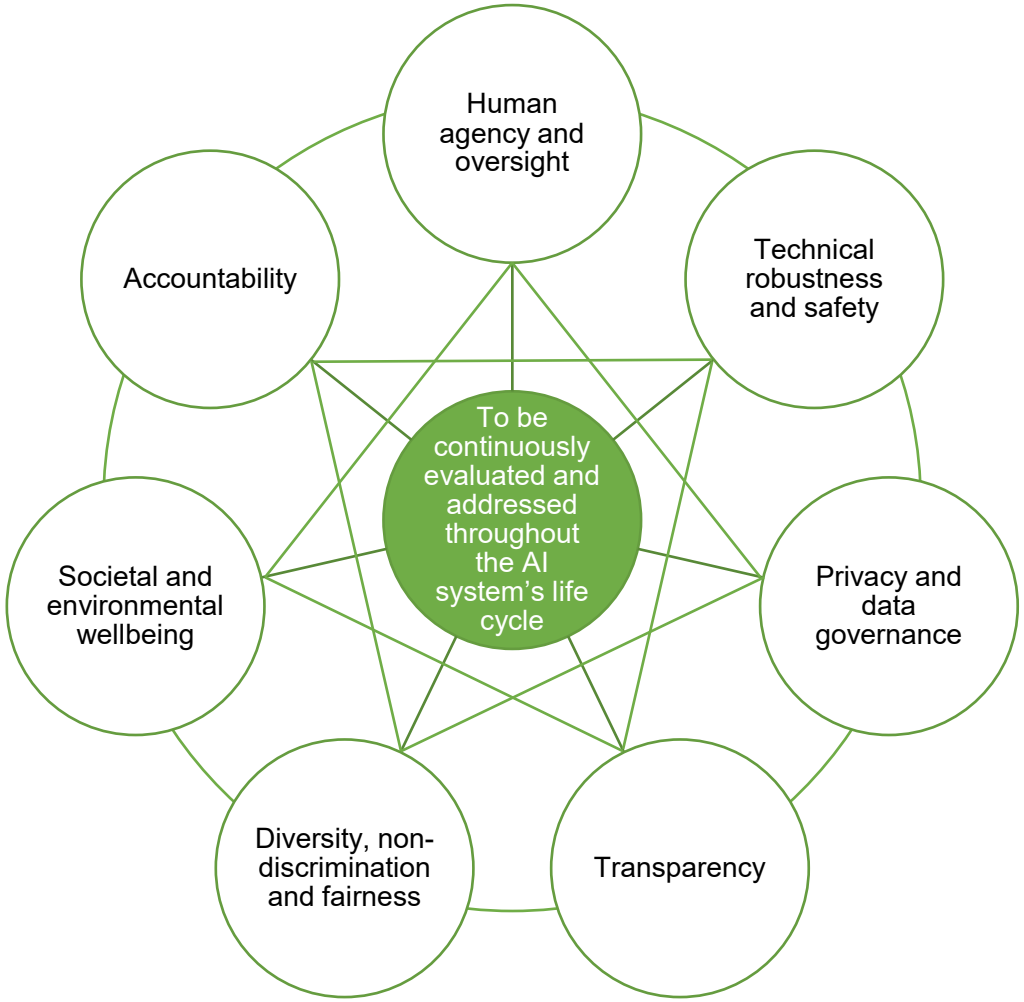
Four Principles of Explainable Artificial Intelligence

P. Jonathon Phillips
Carina A. Hahn
Peter C. Fontana
David A. Broniatowski
Mark A. Przybocki

This draft publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8312-draft

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Development of Industry Standards



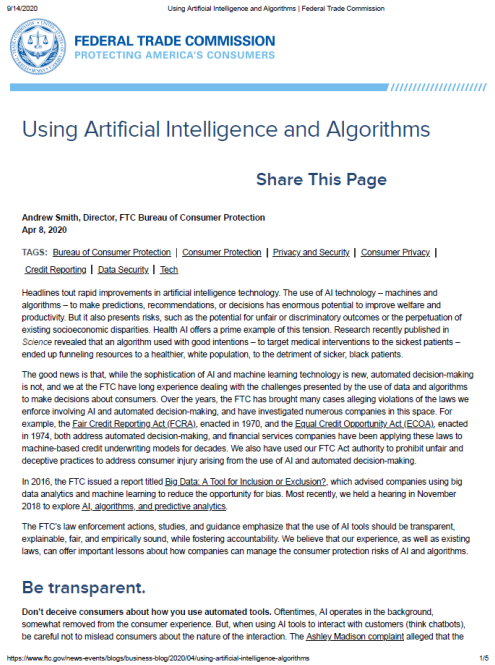
E.C. AI Ethics Guidelines
Figure 2

Interrelationship of the seven requirements: all are of equal importance, support each other, and should be implemented and evaluated throughout the AI system's lifecycle

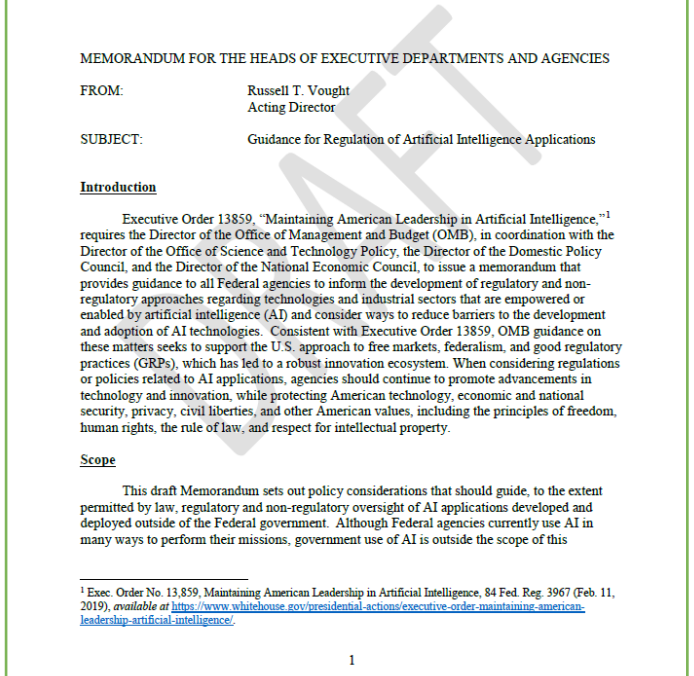
Developments in the US

FTC: Big Data (Jan. 2016)

FTC Using AI and Algorithms (Apr. 2020)

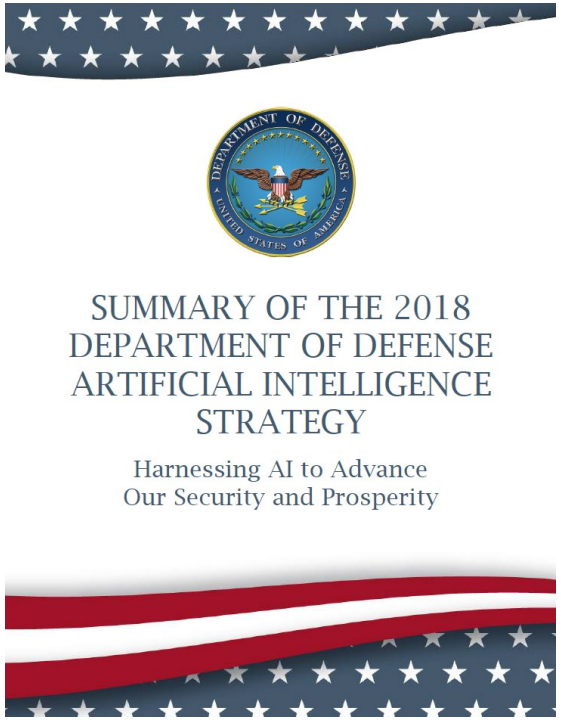


White House AI Principles (Jan. 2020)



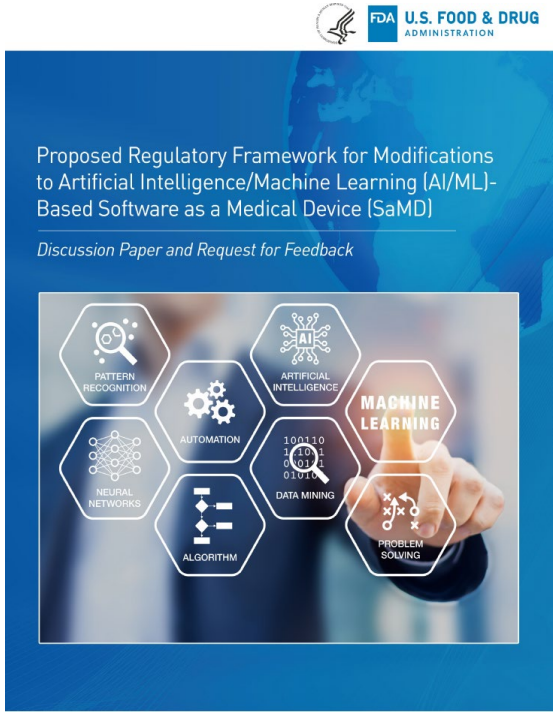
Developments in the US

DOD AI Strategy (2018)



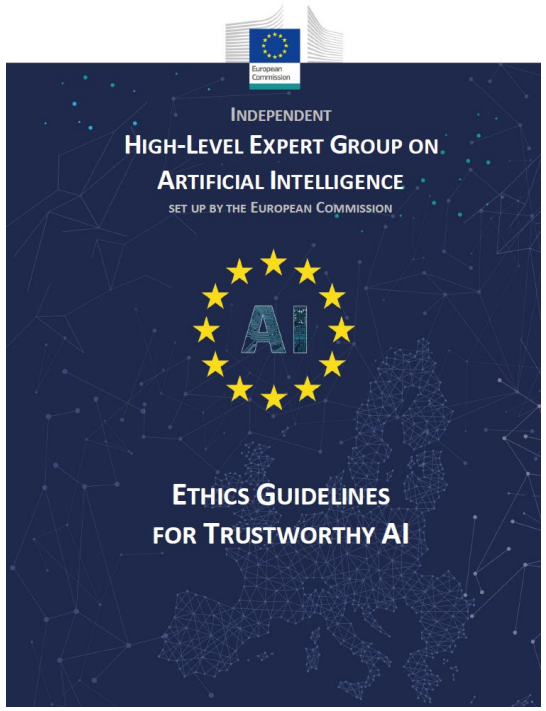
FINRA - AI in the Securities Industry (June. 2020)

FDA: AI in Medical Devices (Apr. 2019)

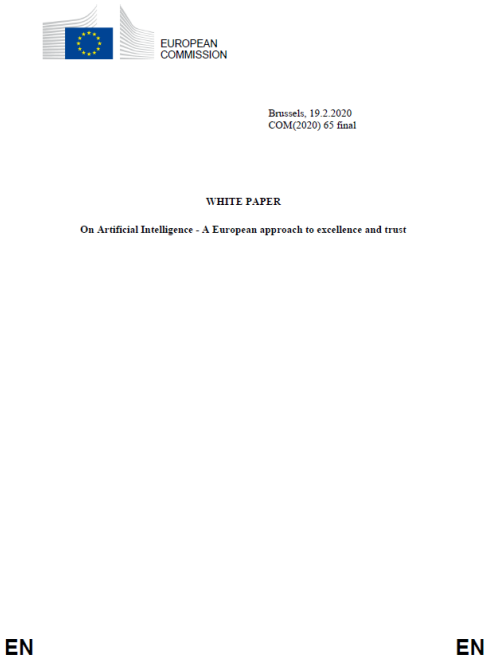


Developments in the EU

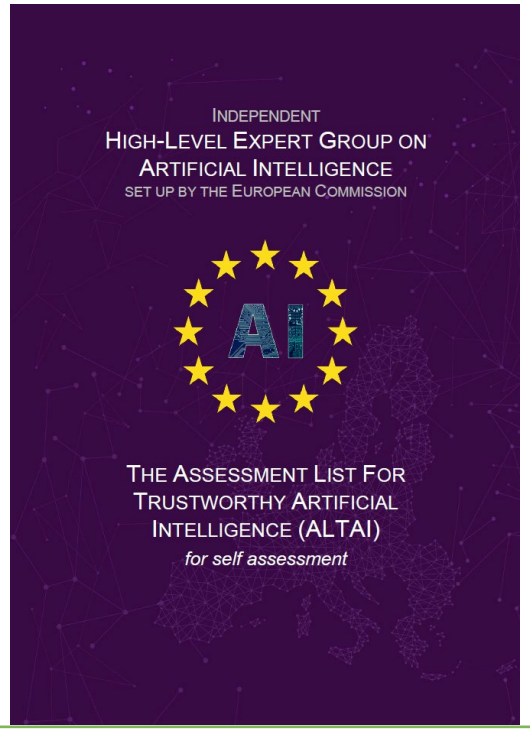
E.C. AI Ethics Guidelines (Apr. 2019)



E.C. Whitepaper on AI (Feb. 2020)

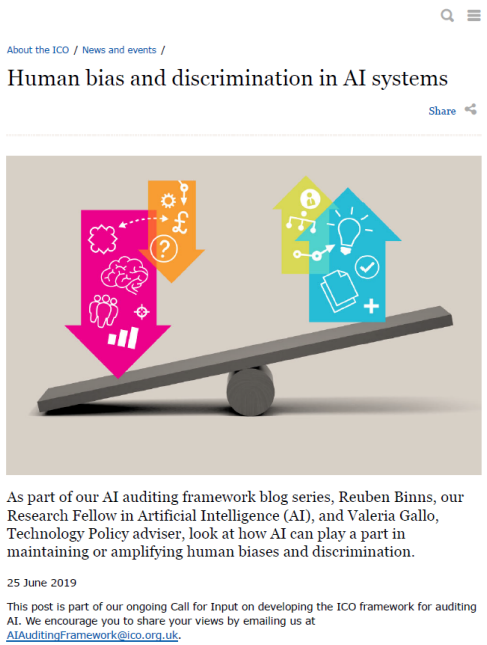


Assessment List for Trustworthy AI (Jul. 2020)



Developments in the UK

Human bias and discrimination in AI (Jun. 2019)



About the ICO / News and events /

Human bias and discrimination in AI systems

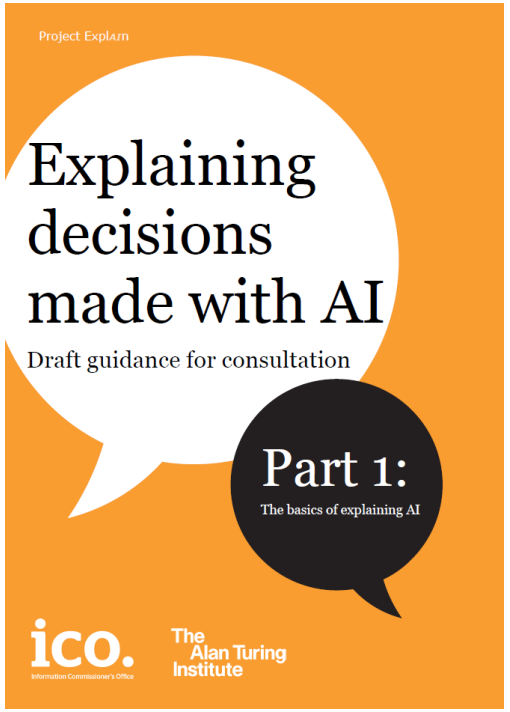
Share

As part of our AI auditing framework blog series, Reuben Binns, our Research Fellow in Artificial Intelligence (AI), and Valeria Gallo, Technology Policy adviser, look at how AI can play a part in maintaining or amplifying human biases and discrimination.

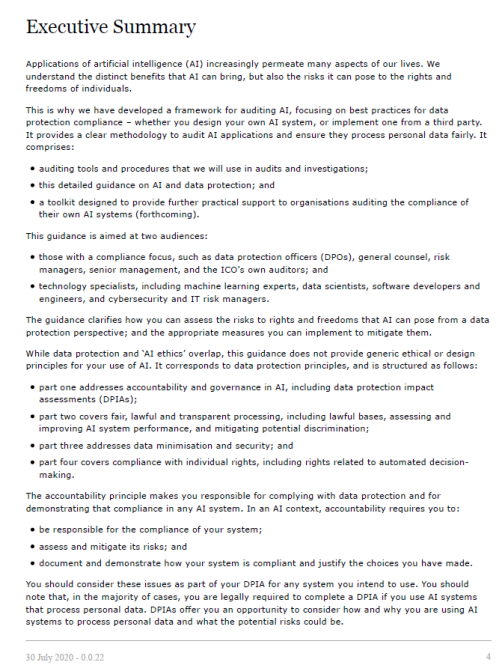
25 June 2019

This post is part of our ongoing Call for Input on developing the ICO framework for auditing AI. We encourage you to share your views by emailing us at AIAuditingFramework@ico.org.uk.

Explaining decision made with AI (Dec. 2019)



AI and data protection (Jul. 2020)



Executive Summary

Applications of artificial intelligence (AI) increasingly permeate many aspects of our lives. We understand the distinct benefits that AI can bring, but also the risks it can pose to the rights and freedoms of individuals.

This is why we have developed a framework for auditing AI, focusing on best practices for data protection compliance – whether you design your own AI system, or implement one from a third party. It provides a clear methodology to audit AI applications and ensure they process personal data fairly. It comprises:

- auditing tools and procedures that we will use in audits and investigations;
- this detailed guidance on AI and data protection; and
- a toolkit designed to provide further practical support to organisations auditing the compliance of their own AI systems (forthcoming).

This guidance is aimed at two audiences:

- those with a compliance focus, such as data protection officers (DPOs), general counsel, risk managers, senior management, and the ICO's own auditors; and
- technology specialists, including machine learning experts, data scientists, software developers and engineers, and cybersecurity and IT risk managers.

The guidance clarifies how you can assess the risks to rights and freedoms that AI can pose from a data protection perspective; and the appropriate measures you can implement to mitigate them.

While data protection and 'AI ethics' overlap, this guidance does not provide generic ethical or design principles for your use of AI. It corresponds to data protection principles, and is structured as follows:

- part one addresses accountability and governance in AI, including data protection impact assessments (DPIAs);
- part two covers fair, lawful and transparent processing, including lawful bases, assessing and improving AI system performance, and mitigating potential discrimination;
- part three addresses data minimisation and security; and
- part four covers compliance with individual rights, including rights related to automated decision-making.

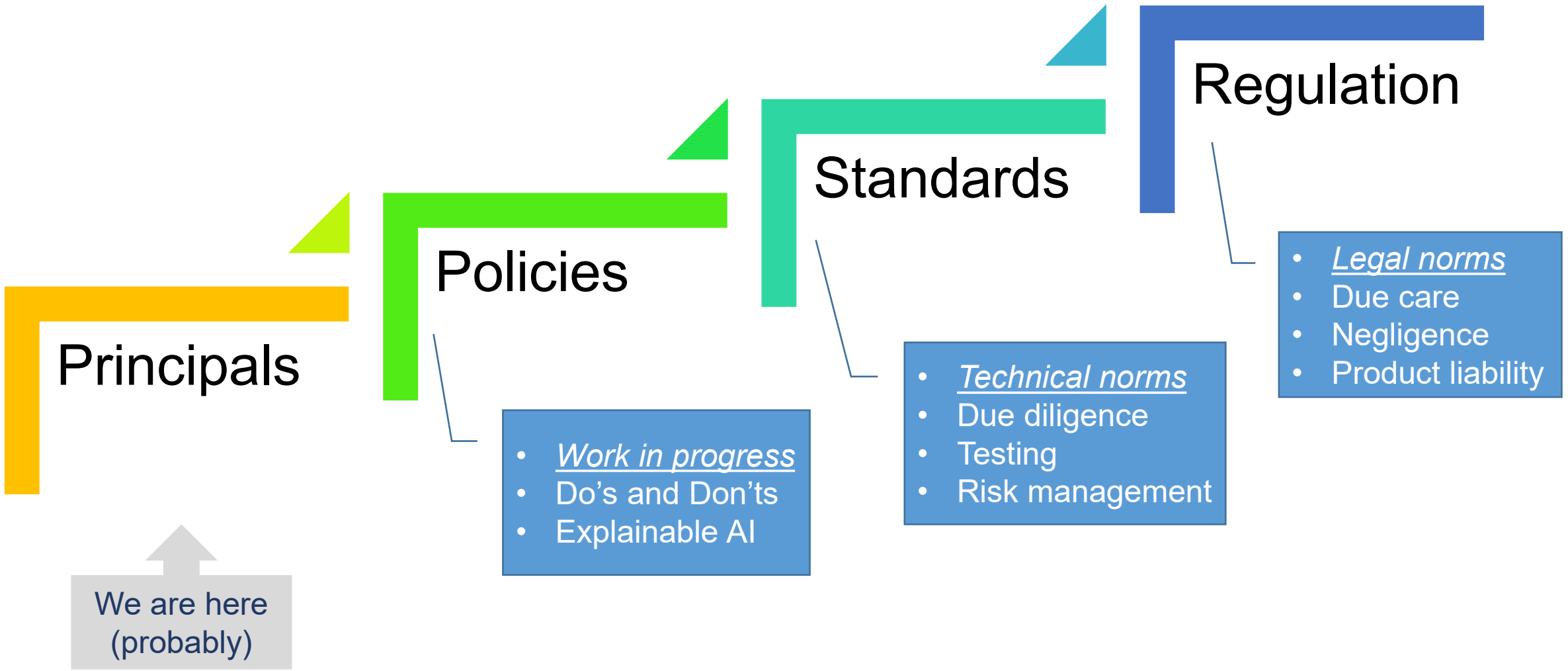
The accountability principle makes you responsible for complying with data protection and for demonstrating that compliance in any AI system. In an AI context, accountability requires you to:

- be responsible for the compliance of your system;
- assess and mitigate its risks; and
- document and demonstrate how your system is compliant and justify the choices you have made.

You should consider these issues as part of your DPIA for any system you intend to use. You should note that, in the majority of cases, you are legally required to complete a DPIA if you use AI systems that process personal data. DPIAs offer you an opportunity to consider how and why you are using AI systems to process personal data and what the potential risks could be.

30 July 2020 - 0.0.22 4

Conceptual approach



Parting thoughts

Learn from cyber!

- It's about risk management
- People, Process, Technology
- Expectations will grow over time
- Guidance → Standards → Laws

Mark Francis

New York

212.513.3572

mark.francis@hklaw.com

Mark Francis is a tech & data partner at the law firm Holland & Knight LLP in New York, with a focus on cybersecurity, data privacy, intellectual property and emerging technology. Mark's practice spans counseling, legal compliance, regulatory investigations, litigation, and a wide array of transactions.

Mark's cybersecurity and privacy practice includes information governance, third party risk management, federal, state and foreign privacy laws, adtech, artificial intelligence, and data assets. He frequently counsels clients in response to data breaches and other incidents, guiding them through internal investigations, regulatory inquiries, and legal disputes.

Mark has a background in computer science and telecommunications, and received his JD/MBA from Fordham University. He is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH), as well as an IAPP CIPP/US, CIPT, and Fellow of Information Privacy. Mark is currently serving on the board of the New York Metro InfraGard association.

https://www.linkedin.com/in/markhfrancis/

HK

Data Strategy, Security & Privacy

Mark Francis | Partner, New York | 212.513.3572 | mark.francis@hklaw.com