University of Illinois at Urbana-Champaign
Dept. of Electrical and Computer Engineering

ECE 101: Exploring Digital Information Technologies for Non-Engineers

Ethics, Fairness and Privacy

Ethics—Foundational Principle

- System of moral principles that guide behavior and decision-making.
- Helps define what is considered right or wrong, good or bad, just or unjust.

Morality Depends Strongly on Culture

But … what are moral principles?

Across human cultures,

- there are **a few common themes**.
- For example, **don't kill people** from your village.

But **otherwise, "morals" can be variable**.

Who Keeps Companies Ethical?

Corporate actions

- are **governed by people**,
- **but** individuals do **not always**
- apply **personal ethos**
- in a competitive setting.

- Meta documents (https://www.npr.org/2026/02/18/nx-s1-5717117/zuckerberg-testimony-social-media-addiction-trial):
  - "If we wanna win big with teens, we must bring them in as tweens,"
  - … from 2015 showed how an estimated 30% of 10- to 12-year-olds in the U.S. were using Instagram.
  - …The company had a goal to increase the time 10-year-olds spend on Instagram

Only Government Can Limit Companies

Bottom line: **ethical business behavior**

- **defined by law and policy**,
- **interpreted by judiciary**, and
- **enforced by government**.

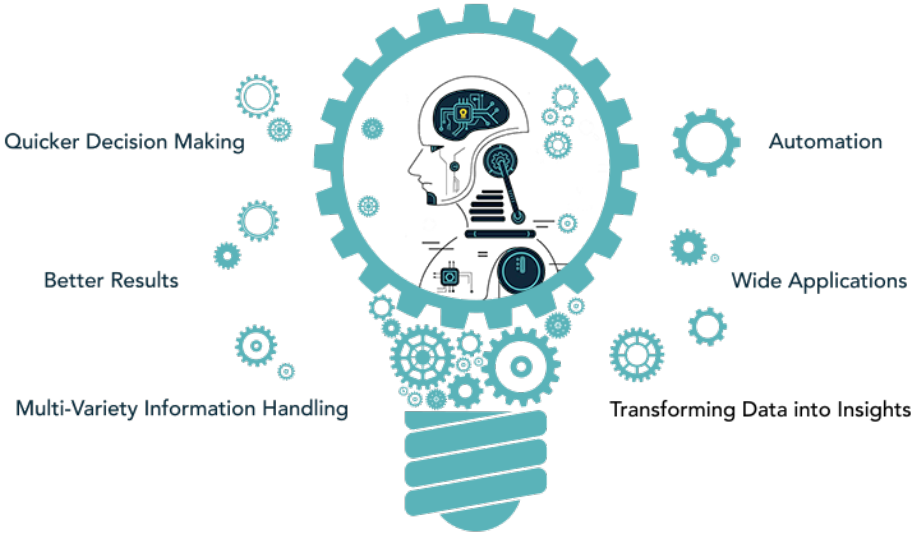
In a democracy, **all** of these **start with you**.

Machine Learning has its Advantages

For any given task, **we can compare use of ML with** use of **human employees**.

Advantages of using ML over humans:

- **Capital costs lower**.
- Usage more **flexible** (same chip executes almost any task, unlike skilled humans).
- **Operating costs** much **lower** (and go down rather than up in off-peak hours).
- **Operates 24/7** in absence of failure.



More Advantages

More advantages of using ML over humans:

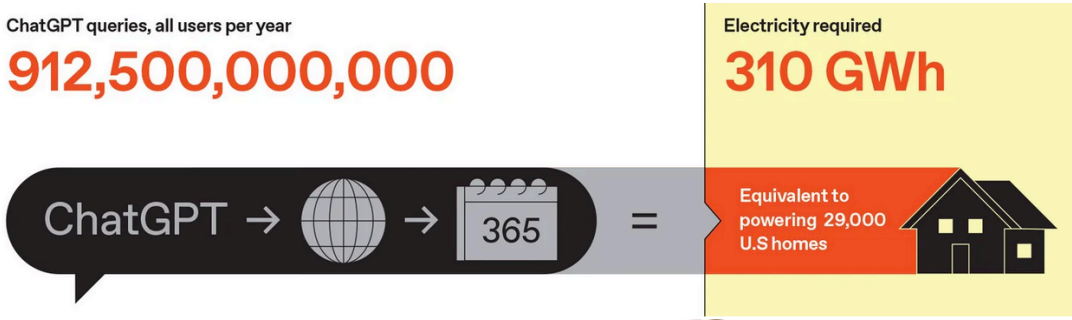
- **Lower failure rate**.
- **No psychological issues**.
- **Minimal safety issues** (only downtime and replacement cost).
- **Replication and replacement nearly instantaneous**.
- **Lightweight and portable** (can fit on a drone or a variety of other robots that can reach places humans generally cannot).

But there are Disadvantages as well

Disadvantages of using ML:

- **Requires** electrical **power**.
- **Results may not be as good** (balance against advantages).

https://spectrum.ieee.org/ai-energy-use



Another **major disadvantage:** decisions **not explainable**.

- Can't learn from ML models.
- No "reason" for results, correct or otherwise.

Who is Responsible for ML Decisions?

Since results generated by ML are not explainable,

who is responsible for actions based on ML-controlled agents?

Let's say an autonomous car.

Many Answers, but Perhaps Not Many Good Ones

- the car owner (possibly in the car)
- the car passenger(s), if any
- the car manufacturer
- the company and/or person(s) who developed the ML model

(maybe most people would stop here?)

Who is responsible for actions based on ML-controlled agents?

- the company that fabricated the chip used to execute the ML model
- the company and/or person(s) who designed the chip used to execute the ML model
- the company and/or person(s) who wrote simulations for producing training data
- the company and/or person(s) who supplied data for writing simulations for training
- the company and/or person(s) who designed the algorithm for learning
- the company and/or person(s) who designed the algorithm for executing the model

Legal Decisions Made by Humans

ML failures will lead to both criminal cases and civil litigation.

In many such cases,

- **juries make decisions**.
- Jurors are **unlikely to have** much technology **expertise**.

Are humans capable of avoiding the assumption that technology is unbiased and infallible, especially with (one side's) lawyers arguing that such is the case?

HUMANS TEND TO AVOID CONFLICT WITH TECHNOLOGY

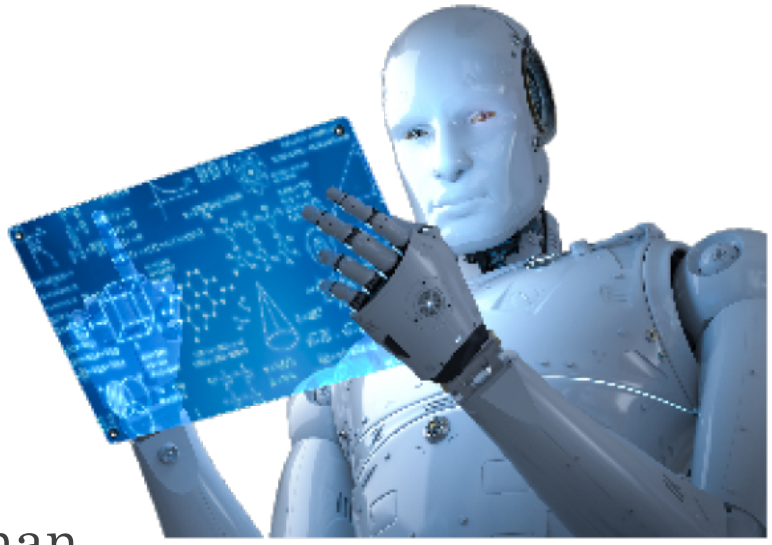
Fairness—An Ethical Value

- Impartial and just treatment without favoritism or discrimination.
- Ensuring equitable outcomes and opportunities for all individuals or groups.

Machine Learning is Mostly Learning by Example

Primary technique for machine learning:

- **start with** a set of **labeled examples**,
- **train a model** to produce the labels, then
- **evaluate** using more labeled data.



As with humans,

- **biases** in data **and absences** of data
- **produce biased / partial models**.

Unlike humans, training is much more costly than evaluation, so **learning** is typically **not continuous**.

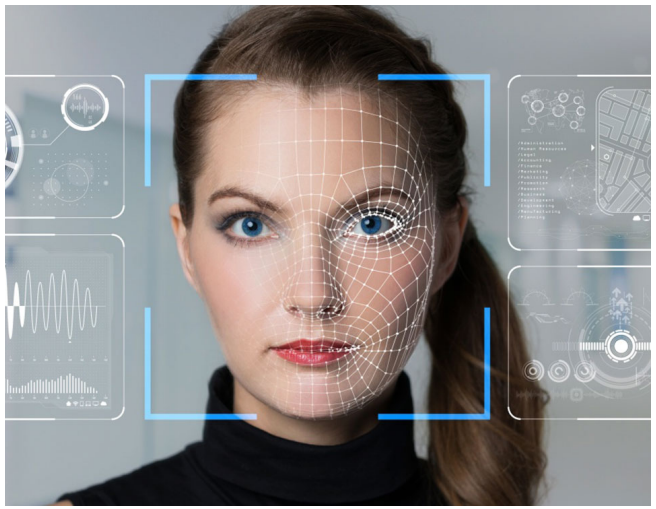
HOW AI WORKS

TRAINING DATA & BIAS

New Technologies Unlikely to be Understood

ML-based face recognition:

- Phones allow it now for unlocking.
  Also used for law enforcement surveillance, airport passenger screening, and employment and housing decisions
- Success rate? 70%? maybe more now …
- What if someone is wearing a mask?
- What if they have a bruise?
- Easy to Misuse and Misrepresent Results from ML



Legislators Identified as Criminals

From Harvard Griffin GSAS science Policy Group

".. over 117 million people, as of 2016 – have photos within a facial recognition network used by law enforcement. This participation occurs without consent, or even awareness, and is bolstered by a lack of legislative oversight."

"…**assessment** of [Amazon] Rekognition's face-matching capability **by** the American Civil Liberties Union (**ACLU**), in which 28 **members of Congress, disproportionately people of color,** were **incorrectly matched with mugshot images**."

Ethical Issues of AI—What are you concerned about?

- AI models can contribute to climate change
- Use of work by artists, authors, creative individuals without their consent; taking away jobs and talents
- AI for school work - not learning the skills
- Deployment can discriminate against entire communities
- Generative AI for images or videos can frame people for things they haven't done
- Lack of trust - what's real whats not
- Friends in AI - pushing people away from friends and society
- Lot of power in the hands of few companies
- Quality of data used training Ai
- Use of AI in government and military

Should Use of AI be Regulated?

Perhaps we should develop standards before allowing use of AI?

- **safer** than the best humans
- **more accurate / correct** than the best humans
- **less biased** than the best humans

(These may not be easy to define and/or evaluate.)

The question of responsibility will still arise, but at least **fewer humans will be harmed**.

Privacy—Application of Ethical Principles

Now, let's consider privacy.

What does the word mean?

Privacy: the state or condition of being free from being observed or disturbed by other people

Privacy vs. Surveillance and Control

Why might someone else want to "observe or disturb" you?

Two reasons:

- **surveillance**: to know what you are doing (the reason could be good, bad, or in between), **and**
- **control**: to influence, limit, or manage your actions.

he right of individuals to control their personal information and protect it from misuse

When are Surveillance and Control Acceptable?

To decide whether such activities are acceptable, we can start with these questions:

- **When** and to what extent **does** government or **someone** else **have the right to monitor your actions?**
- **When** and to what extent **does** government or **someone** else **have the right to control what you are allowed to do?**

"Never" is Not the Right Answer

You may be tempted to answer, "Never."

But that's not a good answer.

Am I allowed

- to come into your apartment as I please and
- use your television,
- eat your food, and
- so forth?

So you want to monitor my behavior, control me, and perhaps even disallow my visits?

You probably even expect me not to visit unless you explicitly invite me to do so.

"The right to swing my fist ends where the other man's nose begins."

– Oliver Wendell Holmes Jr.

Both Culture and Politics Affect the Answers

Ethical considerations around privacy often involve balancing individual rights with societal or organizational needs

Between

- "Who controls you in your private space?" and
- "Who controls you in another person's private space?"
- is a huge gray area.

Answers vary both culturally and politically.

Control Example: Internet Service Providers

Let's focus on a control question.

If you buy Internet service from my company, am I allowed to …

- Limit your bandwidth?
- Limit your bandwidth for specific applications?
- Prevent or restrict you from accessing some services?
- Sell your ability to access services to someone else? (In other words, only allow you to make use of services that pay me.)

Net Neutrality Akin to Freedom of Speech?

THE FLOW OF INFORMATION ON THE INTERNET SHOULD BE TREATED EQUALLY AND THAT INTERNET SERVICE PROVIDERS CAN'T INTERFERE WITH WHAT CONSUMERS DO ONLINE ...

These questions are central to the issue of "**net neutrality**" that has been a topic of recent political discussions.

Do customers have the right to find content and use services that suit their tastes?

What does "free speech" mean if a small number of large companies control what can be "heard" on the Internet?

Net Neutrality—Subject of a lot of Debate

Net neutrality is the principle that Internet Service Providers (ISPs) must treat all internet data equally, without blocking, slowing down, or charging for preferential treatment of specific content, websites, or applications.

- **2015**: Open Internet order, allowed FCC to ban practices like blocking content or giving preference to some kind of content over others
- **2017** repealed: Government overreach, was killing innovation and competition in broadband industry
- **2024** reinstated
- **2025** struck down by court; FCC does not have the legal authority to impose national net neutrality rules on broadband providers.
- States like California, Washington, and Oregon have their own laws

Should Control be Left to the Service Provider?

The same questions might be asked about other services, too.

Consider the same question

- in terms of search engines:
- **is a search engine allowed to sell your ability to find URLs?**

In other words, is it acceptable to put paid advertisements at the top of a search response?

As the only response?

Does Payment Matter? Is Internet a Telephony Service?

Would you say "yes" because you don't pay for web search?

It's easy for an Internet service provider to include a control agreement in your contract.

The question is: **should they be allowed to do so?**

What if your cell provider only allowed you to call businesses "in their network" (in other words, businesses who pay the provider)?

Privacy vs. Ethics: Surveillance for your Benefit?

What if the crimes are victimless and unenforced?

About 20 years ago, rental car companies

- installed speed-monitoring chips in their vehicles.*
- Drivers who broke speed limits
  - were charged extra fees, but
  - were not reported to local authorities.

*And told customers about them in the fine print.

Customers Offered a Resounding, "NO!"

Why?

- Lower insurance costs!
- Some of the reduction
  - passed on to customers renting cars
  - (a competitive advantage).

Customers hated it, and the idea vanished.

So What's Your View?

Would you agree to surveillance of your activities in return for lower prices?*

Would you agree to 24/7 monitoring of your location and actions in return for … ?

*Assume no illegal use of collected data.
But do you know what's legally allowed?

Surveillance Example: Dystopian Future

Minority Report is a sci-fi movie showing very believable technology about data collection and its use.

- Citizens have eye implants scanned by surveillance robots (like spiders) and security cameras
- Citizens receive tailored recommendations in shopping mall
- Do not need tickets on the subway
- Allowed to pass through security checks
- A criminal is unable to hide from law enforcement

Surveillance: Location and Interests

Surveillance can cause problems, even in the absence of crime.

Typically, monitoring collects things like

- location,
- motion,
- interests,
- comments/ideas, and
- events attended.

Information may be sensitive.

Surveillance Information can be Crowdsourced

Information can also be gathered
- from many anonymous people,
- using **crowdsourcing**

Map apps allow users to report slowdowns (automatically!), accidents, construction, speed traps, and so forth.

All users on roads contributed information.

Improve travel planning for everyone!

Completely impersonal, right?

Crowdsourced Information can be Powerful

Why did someone write this app?

To be kind and generous?

Maybe.

Early versions included an app was written by a former intelligence agent.

Say that you want to know

- the location of a visiting state dignitary
- (not generally public information).

Would it be hard to find major traffic obstructions unrelated to accidents, construction, and so forth, and correlate those with the visitor's general locale?

Surveillance Data for Machine Intelligence

Example: Machine Learning used for Fraud Detection

Travel tracking vs. identify theft

You purchase an airline ticket.

Who knows about it? Are you under surveillance?

- Your **credit card company** (bill sent to them with information about passengers, etc., for fraud detection)
- Your **email provider** (confirmation email analyzed for travel plans—your name AND your companions)

Surveillance Information Reduces Fraud and Improves Services

When you travel, **these companies** (and others) **can tell where you are.**

Credit card **purchases include geographical information**.

If you buy a ticket to Hawaii

- and try to make a "purchase" in-person in Florida,
- most credit cards will decline the purchase.

Any **use of** the **Internet** (WiFi) **includes a local IP address** that can be used to identify your location.

Will You Trade Your Privacy for Such Benefits?

Would you allow your credit card company to inspect your web history to provide better fraud detection?

Would you (do you) make use of builtin/ plugin lists of web sites that are "dangerous" in terms of likely virus attacks?

Terminology You Should Know from These Slides

- ethics
- fairness
- learning by example
- model bias and error
- privacy
- surveillance
- control
- net neutrality

Concepts You Should Know from These Slides

- how does bias creep into machine learning data
- advantages and disadvantages of ML
- lack of explainability for ML results
- societal assumptions about technology (and differences with reality)
- commercial and legal value of surveillance and control
- potential benefits of allowing use of personal information
- impact of politics and governmental self-interest on privacy, law, and business