Accountability in Digital Technology: Why It's Lacking and How to Fix It

Digital technologies and AI systems increasingly shape our lives – from what news we see, to how companies make decisions about us. Yet when these powerful tools cause harm or behave unfairly, **who is held accountable?** Today, **legal accountability in tech is alarmingly weak**. Below we explore why this is the case – and how we can change it – focusing on four key issues:

1. **Lack of Universal Standards**
2. **Dominance of Tech Giants**
3. **Absence of Accountability Mechanisms**
4. **Solutions: Standards, Penalties & Public Disclosure**

Each section presents the problem and cites real reports and examples, before concluding with solutions to ensure technology serves the public interest, not just corporate profit.

1. Lack of Universal Standards

No common rulebook. Unlike older industries (e.g. food or aviation) that follow strict standards, the tech industry largely regulates itself. Each company develops its **own internal AI ethics guidelines** and procedures, resulting in a patchwork of rules. There is **no single, universally accepted framework** to guide AI decision-making across the board. A UN forum on AI governance noted the urgent need to translate *"global considerations... into concrete industrial standards"*

unido.org
– but so far, that hasn't happened. **Industry conferences and alliances** (such as a recent UNIDO Global AI forum) are actively debating how to set common governance frameworks and quality standards
unido.org
, which shows the need for a unified approach. However, in practice, companies still march to their own drum.

Fragmented and inconsistent. The result of this standard vacuum is *fragmented accountability*. What one company flags as "unethical AI" might be business-as-usual for another. A U.S. government analysis highlighted a *"current dearth of consensus technical standards"* for evaluating AI systems – a major barrier to assuring these systems are safe and fair

ntia.gov
. In fact, these *"under-developed standards mean uncertainty"* for companies trying to comply, and **reduced assurance for the public** that AI is being used responsibly
ntia.gov
. Simply put, without common standards, it's hard to even define what "accountability" means, let alone enforce it.

Voluntary guidelines aren't enough. There have been attempts to create global principles – for example, **all 193 UNESCO member states adopted an AI Ethics Recommendation in 2021** with values like transparency and accountability

computerweekly.com
. But that recommendation is **non-binding**. Similarly, the OECD's international AI principles (endorsed by 42 countries) set lofty goals for **"robust, safe, fair and trustworthy"** AI
nextgov.com
, yet rely on voluntary adoption. In absence of legal force, tech companies can cherry-pick which guidelines to follow. This leaves **significant gaps**. One country's or company's "AI ethics panel" might have strict rules, while another's has none. Such inconsistency makes it easy for bad practices to slip through cracks. **No universal standards = no universal accountability.**

2. Dominance of Tech Giants

A handful of "Big Tech" corporations dominate AI and digital services, giving them outsized power to set the industry's rules (logos of Google, Apple, Meta (Facebook), Amazon, and Microsoft pictured).

Monopolies and self-rule. The digital technology sector today is often described as a **monopoly or oligopoly** – essentially, *a few giant firms control the market*. Whether it's social media, online retail, mobile operating systems, or cloud AI services, a short list of names keeps appearing. Because these giants face little competition, they also face **little external accountability**. They more or less **set their own rules** for how their platforms operate. As the Vice Chair of a U.S. House Antitrust panel put it, *"unregulated tech giants have become too big to care and too powerful to ever put people over profits"*

democrats-judiciary.house.gov
. In other words, these corporations often prioritize growth and revenue, and **there's scant oversight** to compel ethical behavior when it doesn't align with their interests.

Profit over responsibility. Investigations have shown how Big Tech firms exploit their dominance. A 450-page Congressional report found that **dominant platforms abuse their monopoly power** *"to destroy competition, exploit other businesses, harm consumers, and impede disruptive innovation"*

democrats-judiciary.house.gov
. For example, Amazon has been accused of using data from small sellers on its platform to launch competing products, and Google has been found to leverage its control of search and mobile systems to favor its own services
democrats-judiciary.house.gov
. These practices tilt the playing field in their favor. And because these companies dominate their domains, **users and smaller businesses have little choice** but to accept their terms. The tech

giants essentially act as **gatekeepers** of the digital world – without accountability, they get to decide who wins, who loses, and what rules apply.

Limited oversight. Another issue is that government regulators struggle to keep up with Big Tech's rapid expansion and complexity. In many countries (notably the US), laws **lag behind** the tech, and enforcement is weak. Big Tech companies are known to aggressively lobby against new regulations, often **shaping the narrative on their own terms**. They fund industry research, set up self-governing ethics boards, and announce "AI principles" of their own – all while resisting outside oversight. The end result is that a handful of CEOs and boards in Silicon Valley make decisions with global impact, with **minimal democratic control**. When those decisions lead to harmful outcomes (privacy violations, misinformation crises, anti-competitive behavior), there is no neutral referee readily stepping in. This **concentration of power** without accountability is dangerous: it means **tech giants effectively police themselves**, usually with the goal of avoiding bad press or boycotts, rather than truly answering to the public or law.

3. Absence of Accountability Mechanisms

"Move fast and break things" – and face no consequences. In the tech world, the mantra of relentless innovation often comes at the cost of safety and ethics. What happens when a social media algorithm amplifies hate speech that leads to real-world violence, or when an AI used in hiring discriminates against women or minorities? Today, *usually nothing happens to the company responsible.* There are **few legal or financial penalties** in place for such harms. As one digital rights watchdog observed, many of the most powerful algorithms in use are *"accountable to no one — not even the companies that build and deploy them."*

rankingdigitalrights.org
Companies might pledge to be "ethical," but if those promises are broken, there is **no clear accountability** – no laws broken, no fines, no executives held responsible.

Real-world harms, no real punishments. We've already seen multiple cases of tech gone wrong with **minimal repercussions** for the culprits:

- *Self-driving car tragedy:* In 2018, an Uber self-driving test vehicle fatally struck a pedestrian. It was the first death caused by an autonomous car. Yet prosecutors found *"no basis for criminal liability"* for Uber itself

  venturebeat.com

  – instead, they pursued charges against the back-up safety driver. The incident exposed how immature oversight is: a cutting-edge AI driving a 2-ton vehicle on public roads presented *"fatal risks"* but had *"minimal oversight from regulators."*

  venturebeat.com

  In the end, Uber faced essentially no penalty for a death caused by its technology.

- *Social media and genocide:* In Myanmar, Facebook's algorithms famously **amplified hate speech** against the Rohingya minority, fueling a horrific campaign of ethnic violence. U.N. investigators concluded in 2018 that Facebook played a *"key role in spreading hate speech that fueled the violence."*

  reuters.com

  The response? Facebook apologized and removed some bad actors, but no one at the company was held accountable for the outcomes. Years later, Rohingya refugees are suing Facebook for $150 billion in damages

  reuters.com

  , but this is after tens of thousands were killed or displaced. There were **no enforceable mechanisms in place in time** to prevent or punish the platform's negligence.

- *Data abuse and privacy violations:* The Cambridge Analytica scandal revealed that Facebook allowed millions of users' data to be harvested and used to manipulate elections. Public outrage led to hearings and pledges to do better. The **legal consequence**? Facebook paid a record **$5 billion fine** to the U.S. FTC for deceiving users about privacy

  theguardian.com

  . $5 billion is a huge number – yet for Facebook it amounted to about a month's revenue, a financial slap on the wrist. After paying the fine, Facebook's business went on as usual. To critics, this looked like **the cost of doing business**, not true accountability.

- *Algorithmic bias:* Numerous studies have found AI systems exhibiting bias – from facial recognition falsely identifying black people as criminals, to job recruitment algorithms downgrading women's résumés. These biases can **cost people opportunities and freedoms**, but companies often face no direct consequences when found out. At most, they might quietly fix or scrap the biased tool after media exposure. There's often **no law clearly broken** by a biased algorithm (unless it violates a specific anti-discrimination law), so no regulator steps in. The individuals harmed can rarely seek redress because it's hard to prove algorithmic discrimination under current laws.

Why impunity prevails. In summary, today's tech landscape has **huge accountability gaps**. Ethical AI guidelines exist on paper, but **they aren't enforceable**. If a company violates its own ethics policy or some industry "best practice," there is no regulator to fine them or court to sentence them – because those guidelines aren't laws. Many harmful practices (like designing addictive apps, or using dark patterns to trick users) fall into legal grey areas. And even when companies do clearly cross a line, they often negotiate settlements without admitting guilt. The **imbalance of power** is such that users and the public bear the brunt of tech's mistakes, while companies escape serious accountability.

Digital technologies are amazing – they power innovation and convenience that were unimaginable just years ago. But **powerful tech without accountability is a recipe for abuse**. We've seen what happens when industry giants play by their own rules and no one else is watching. To protect consumers, competition, and our fundamental rights, we must weave **accountability into the fabric of the digital world**. That means **setting universal standards**, **reining in monopolistic power**, **creating real consequences for harm**, and **demanding transparency** at every turn. The good news is that momentum is building: governments are waking up to Big Tech's excesses, international bodies are pushing for cooperation, and citizens are increasingly vocal that tech companies *"do the right thing."* It will take smart policy and persistent public pressure, but accountability in tech is achievable.

In the end, **technology should serve humanity – not the other way around**. By implementing the solutions above, we can ensure that digital innovation doesn't come at the expense of ethics and responsibility. The time of tech's wild west is waning. It's time to hold the digital industry to the same standards of accountability that we expect in any other domain. When we do, we'll build a safer, fairer digital future where trust in technology is well-earned, and those who deploy powerful tools are answerable for their impact on society.

Algorithms, Bias, and Accountability: Why the Myth of Neutrality is Dangerous

Introduction

Many people assume that computer algorithms are perfectly neutral decision-makers. After all, algorithms are just math and code – how could they possibly be **biased**? This misconception leads us to trust algorithmic choices as fairer or more objective than decisions made by humans. In everyday life, we often cede judgment to technology without question. For example, given a hard task, people tend to rely more on a computer's recommendation than a person's advice, believing the machine will be more accurate

sciencealert.com

. We see algorithms as cold, logical engines free from human error or prejudice. However, this blind faith in technology can be misguided and even dangerous
sciencealert.com
. In reality, algorithms reflect the people and data behind them – and they **can** and **do** make biased, unfair, or flawed decisions. Understanding this truth is critical, because treating algorithms as infallible robs us of accountability when things go wrong.

The Illusion of Neutrality

Why do so many of us assume algorithms are impartial? Part of it is the **"mechanical mystique"** – the notion that because a computer program follows set rules, it will apply them equally to everyone and everything. We hear phrases like "the computer doesn't lie" or "it's just the algorithm," which foster the belief that algorithms operate without subjective influence. It's similar to the old saying, **"guns don't kill people; people do."** In other words, an algorithm is seen as a neutral tool – any harm must come from a bad user, not the tool itself. This mindset leads to an **accountability vacuum**, where creators of algorithmic systems deflect responsibility by pointing at the machine.

Tech companies have often leaned on this illusion of neutrality to escape blame. When the Apple Card's credit algorithm was accused of offering drastically lower credit limits to women than men, the issuing bank (Goldman Sachs) immediately denied any wrongdoing. **"There isn't any gender bias in the algorithm,"** Goldman insisted, noting that the model didn't even use gender as an input

wired.com
. In essence, they argued the algorithm was **"blind"** to gender and therefore could not be discriminatory – a convenient defense that sidestepped deeper questions. No one from Apple or Goldman could fully explain how the automated credit decision system worked, yet they were quick to trust it as impartial and absolve themselves
wired.com
. This is a prime example of the neutrality myth in action: by portraying the algorithm as an objective judge, the company attempted to dodge accountability for the biased outcomes. We've seen similar tactics elsewhere, from social media firms blaming "the algorithm" for spreading harmful content to hiring platforms suggesting any bias is unintentional and thus not their fault. The **belief that algorithms are neutral by default** provides a comforting cover for organizations – allowing them to credit the technology for successes but **blame the technology for failures**, as if they had no control over it.

The Reality: Technology is Not Neutral

In truth, **technology is socially constructed**. Every algorithm is created by people – people who decide what the algorithm should do, what data it will use, and what **"success"** looks like. As a result, **human values and biases are baked in** at every step

algorithmwatch.org

. An AlgorithmWatch analysis puts it plainly: algorithms and AI systems *"are neither objective nor neutral but outcomes of human deliberation and power struggles."* They embed the judgments, priorities, and blind spots of their designers
algorithmwatch.org

algorithmwatch.org
. Even machine-learning algorithms that *teach themselves* patterns from data are not escaping human influence – because the **data itself comes from our society**, with all its inequities. As the U.S. National Institute of Standards and Technology (NIST) noted in a 2022 report, a great deal of AI bias **stems from human and institutional biases** present in the real world
nist.gov
. In short, if you train an algorithm on biased data, it will likely reproduce or even amplify those biases
algorithmwatch.org
.

Figure 1: An illustration of bias in AI from NIST shows an iceberg analogy – the visible "statistical" biases in an algorithm rest on a larger mass of hidden **human and systemic biases** beneath the surface
nist.gov
. In other words, what might look like an impartial computation is built on foundations shaped by society. We cannot pretend that technology exists in a vacuum separate from human influence.

Because of this, **technology can never be purely neutral.** In practice, algorithms often end up reflecting and reinforcing existing prejudices or serving the interests of those who deploy them. There are countless real-world examples across industries:

- **Hiring:** Amazon developed an AI recruiting tool intended to rate job applicants objectively. But the tool learned from the company's past hiring data – which was predominantly male – and taught itself that male candidates were preferable. Resumes mentioning "women's" (as in women's sports or organizations) were down-ranked, and female candidates were unfairly penalized

  reuters.com

  . What was supposed to be a merit-based algorithm turned out to replicate gender bias in hiring. Amazon had to scrap the project once they realized it "did not like women"

  reuters.com

  reuters.com

  .

- **Search and Social Media:** Algorithms used by online platforms have also exhibited bias. Google, for instance, faced criticism when its auto-complete and image recognition algorithms produced racist and sexist results (e.g. offensive search suggestions or mis-identifying people of color)

  wired.com

  . These issues arose because the algorithms learned from historical online content and user behavior, absorbing the prejudices present in that data. Similarly, social media feeds and recommendation systems often prioritize sensational or divisive content – not because the algorithms *intend* to spread hate or misinformation, but because they are optimized for engagement and thus reflect whatever grabs attention (often outrage or extreme views). The technology is serving the platform's interest (maximizing user engagement and ad revenue), but unintentionally it can sow polarization or amplify harmful speech.

- **Facial Recognition:** Facial recognition algorithms have been found to be far less accurate for women and people with darker skin tones than for white men

  wired.com

  . Why? Because many systems were trained primarily on datasets of light-skinned male faces, mirroring a lack of diversity in tech development. The result is a technology that is highly accurate for one demographic and markedly error-prone for others – which is anything but neutral. Even tech giants have acknowledged this problem. Microsoft, for example, had a facial analysis service that performed much worse on women and minorities; the company's president Brad Smith cited this as evidence that **both industry and government need to "step up – and act" to ensure AI is used ethically**

  wired.com

  wired.com

  .

- **Predictive Algorithms:** In fields ranging from credit lending to healthcare, predictive models can inherit societal biases. A health algorithm used in U.S. hospitals was found to underestimate the medical needs of Black patients compared to white patients with the same health profile

  wyden.senate.gov

  . It treated race as irrelevant (similar to the "colorblind" approach), but because it used healthcare spending as a proxy for need – and less money is spent on Black patients on

average due to unequal access – the algorithm falsely concluded Black patients were healthier than they really were. Again, the bias was not explicitly programmed (no one wrote "prioritize white patients"), but it emerged from the data and design choices.

All these cases drive home the point: **algorithms reflect the real world – warts and all**. They are not inherently fair just because they are automated. In fact, technologies have long been used to entrench advantages. From redlining in financial algorithms to filter bubbles in social media, we see that algorithms can serve the interests of powerful groups or existing systems, intentionally or not. As one industry commentary put it, an algorithm will subject all inputs to the same rules, **"but obviously that's beside the point"** if the rules themselves or the data are skewed

algorithmwatch.org
.

Consequences of the Neutrality Myth

When society believes the myth that "algorithms are neutral arbiters," the consequences extend far beyond any single case. **Accountability diminishes at every level.** Companies and government agencies can pass the buck to technology, and victims of algorithmic harms struggle to find recourse. Here are some of the key repercussions we've already seen:

- **Corporate Evasion of Responsibility:** The neutrality myth provides a handy shield for organizations: they can always say *"it's the algorithm's doing, not ours."* This mindset was evident in the Apple Card incident, where Goldman Sachs defended itself by claiming the algorithm couldn't possibly discriminate

  wired.com

  . We've also seen social media CEOs, when pressed about harmful content or extremist recommendations, respond that their platforms simply show people what they engage with – as if the algorithm's outputs are an inevitable force of nature. Such deflections allow companies to avoid taking a hard look at their design choices. If a hiring algorithm rejects all the female candidates, a company might quietly shelve the tool (as Amazon did) but frame it as a technical glitch rather than acknowledging **discriminatory design**. Without external pressure, the problems can be swept under the rug. The danger is that biased systems may continue to operate in less obvious ways, unchecked.

- **Lack of Redress for Affected Individuals:** When you're harmed by a biased or faulty algorithm, it can be maddeningly difficult to get accountability if everyone assumes the system is neutral. Several Black men in the U.S. have been **wrongfully arrested** because police relied on flawed facial recognition matches. One man, Robert Williams, was arrested in Detroit in 2020 after an algorithm mismatched his face with surveillance footage of a crime he didn't commit

  fox2detroit.com

. He was detained overnight for a robbery he had nothing to do with. Cases like Williams' occurred because officers placed undue trust in the software's "neutral" judgment. Initially, there was a tendency to blame the identification on the computer and view it as an unfortunate error rather than a civil rights issue. It took lawsuits and public outcry to prompt change. Detroit Police have since revised their policies, barring arrests based solely on facial recognition and agreeing to audits of past cases

fox2detroit.com

. But think about how many individuals might have been falsely flagged or traumatized before these cases came to light. If we keep excusing the algorithm, those individuals are left without an apology, let alone justice.

- **Regulatory Hesitation and Gaps:** Policymakers have also been influenced by the perceived objectivity of algorithms, often adopting a **hands-off approach** in the early days of AI deployment. For years, tech companies enjoyed relatively light regulation under the assumption that digital innovations were generally beneficial and self-correcting. After all, if an algorithm is just "math," why regulate math? This hesitation meant that discriminatory AI systems rolled out in hiring, lending, policing, and other domains faster than laws or oversight mechanisms. In some cases, officials themselves trusted algorithmic systems too readily. In the UK, an exam-grading algorithm in 2020 systematically downgraded students from disadvantaged schools, sparking outrage. Initially, education officials defended the algorithm's results as the best impartial estimate, delaying redress to affected students

  theguardian.com

  . Only after massive student protests (with signs reading "ditch the algorithm") did the government acknowledge the algorithm's flaws and reverse course. The broader point is that **misplaced trust in algorithmic objectivity can make regulators slow to intervene**, even when people are clearly being harmed. Every moment of delay is more damage done – students missing university spots, qualified job seekers passed over, innocent people surveilled or jailed.

- **Reinforcing Social Inequities:** Perhaps the gravest consequence of believing technology is neutral is that it can **entrench systemic biases under the guise of fairness**. When an algorithmic decision system is deployed without accountability, any bias in it tends to compound over time. For instance, predictive policing algorithms like PredPol were sold as data-driven tools to allocate police resources "fairly." In practice, they often sent officers disproportionately to communities of color, because they were trained on historical crime data that reflected over-policing of those areas. Investigative journalists found that PredPol's algorithm **"mostly avoided Whiter neighborhoods"** and instead **flooded Black and Latino neighborhoods with thousands of crime predictions**, sometimes tagging the same areas daily

  themarkup.org

themarkup.org

. This led to **over-policing** – more patrols, more scrutiny, and inevitably more minor infractions recorded in those communities – which then fed the algorithm with more data reinforcing the notion those areas are high-crime. Meanwhile, wealthier (and whiter) neighborhoods enjoyed fewer patrols and even if crime occurred there, it was less likely to be predicted or recorded

themarkup.org

themarkup.org

. All of this was justified under the banner of an "unbiased" algorithm. The neutrality myth thus can mask a vicious cycle of inequality: bias in, bias out – but with a scientific stamp of approval. It takes significant effort (and often external audits or investigative reports) to reveal these feedback loops and hold someone accountable for breaking them.

- **Social and Ethical Backlash:** As more people wake up to these issues, there's a growing public backlash against unaccountable algorithms. The myth of neutrality, once shattered, leads to anger and demands for justice. We saw this with the Facebook scandal in Myanmar. For years, Facebook's leadership insisted that their recommendation algorithms were simply connecting people, neutral with respect to content. In reality, those algorithms amplified hate speech and incitements to violence against the Rohingya minority, contributing to a genocidal campaign

amnesty.org

amnesty.org

. Facebook only admitted problems after evidence mounted that its platform had become an **"echo chamber of hatred"** driven by **"hate-spiralling algorithms"** that kept users engaged by showing inflammatory content

amnesty.org

amnesty.org

. By treating the platform as a neutral medium, the company had avoided timely intervention, with horrific real-world consequences. Amnesty International later blasted Meta (Facebook's parent company), saying **"Meta must be held to account… [it] was profiting from the echo chamber of hatred"** and demanding reparations for the Rohingya victims

amnesty.org

. This is accountability coming belatedly, after irreparable harm. The lesson is that failing to challenge the neutrality myth early can lead to **widespread harm and a crisis of public trust** in technology.

In sum, believing that algorithms are always fair and objective isn't just a harmless misunderstanding – it has concrete impacts. It creates an environment where biased or flawed AI systems can operate without proper oversight. Companies might escape liability, but the people and communities affected do not escape the outcomes. From denied loans and unjust jail sentences to entire populations being targeted or ignored, the costs are high. And when the bubble bursts, as it inevitably does, it erodes trust in all technology. People justifiably feel that they were sold "fairness" and given prejudice. To avoid such outcomes, we must insist on **accountability and transparency** for algorithmic decisions at every step.

Conclusion

In the end, the notion that algorithms are unbiased, neutral decision-makers is a dangerous fantasy. It lulls us into handing over important decisions to systems we don't question – systems created by fallible humans and fed with imperfect data. As we've seen, this **perception of neutrality is not only wrong, it's perilous**. It has allowed discrimination to go undetected in automated hiring and lending, put innocent people in jail, deprived students of earned opportunities, and amplified social injustices under the cloak of "objective" technology. The **myth of the impartial algorithm** serves only those who benefit from lack of scrutiny, while those harmed are left with little recourse.

Dispelling this myth is the first step toward a future where AI works for all of us, not just for the convenience or profit of a few. We must approach algorithms with a healthy dose of skepticism and a firm demand: **"Prove to us that you are fair. And if you're not, we will hold you accountable."** This means insisting on transparency – we should be able to know when an algorithm is making a decision about us and understand how it's reaching that decision. It means insisting on oversight – independent audits, impact assessments, and regulations that ensure AI is held to the standards we expect in a democratic society. And it means keeping humans in the loop – not as a token gesture, but in a meaningful way that allows human values like compassion and equity to guide automated systems, and allows human judgment to overturn algorithmic mistakes.

The **call to action** is clear. As citizens, consumers, and participants in a society increasingly run by algorithms, we need to be aware and vocal. Ask questions: "What data is this algorithm using? Could it be biased? Who takes responsibility if it's wrong?" Support policies and leaders

who prioritize algorithmic accountability. Encourage companies that choose ethics over easy excuses. And educate others – the more people understand that technology is not infallible, the more momentum we build for change.

We stand at a crossroads where we can either be governed by opaque algorithms or ensure that **algorithms are governed by our principles**. By rejecting the myth of neutrality, we affirm that *we, the people*, should ultimately control technology's role in our lives. Let's replace unjust algorithms with just ones, and secrecy with sunlight. In an age of AI, maintaining human accountability isn't a Luddite impulse; it's a necessary safeguard for liberty, equality, and trust. **Algorithms will shape the future – but it's up to us to shape the algorithms.**