ChatGPT

Protocol for Correcting Algorithmic Misclassification and Misprofiling

Formal AI Ethics Protocol (White Paper Style)

Abstract:

Modern AI surveillance and profiling systems can inadvertently misclassify individuals by conflating correlated behaviors or co-located data signals with causative identity traits. This “guilt-by-association” effect results in false profiles that can inflict psychological harm and unjust outcomes [1] [2]. We propose a formal ethics protocol, termed **Systemic Repentance and Correction**, to guide AI developers and organizations in rectifying such errors. The protocol consists of five stages: **Realization** of faults, **Revelation** through transparency, **Reclassification** of erroneous data, **Restoration** for affected parties, and **Recommitment** to ethical practices. Each stage aligns with existing data rights (e.g., transparency, rectification) and emphasizes human-centric, restorative approaches to rebuild trust and integrity in AI systems.

Introduction:

AI-driven decision systems—from social media algorithms to law enforcement tools—are increasingly used to profile human behavior. A critical issue has emerged: algorithms may collapse distinct individuals or contexts into a single “identity vector” based on proximity or association rather than actual agency. In other words, if Person A and Person B share some behaviors or are frequently in the same data context, a model might unjustly treat them as one entity or infer traits of one from the other. Such misclassification violates a fundamental principle of statistics and causality: **correlation does not equal causation**. It also breaches the conditional independence assumptions behind many models (e.g. a Markov model’s state should not indiscriminately merge independent agents). In effect, the AI performs a premature “observation collapse,” conflating separate people’s signals as one—a flawed analogy to collapsing quantum wavefunctions without a valid observer linkage.

This misprofiling by association has real-world consequences. Research and civil rights reports show that crude profiling based on neighborhood, network, or other non-causal criteria can *“ruin lives”* by wrongly labeling individuals as suspicious or high-risk without evidence [1]. For example, police gang databases have included people solely due to their relatives or attire, leading to unjustified surveillance and prejudice [3]. Likewise, commercial algorithms might flag someone as a fraud risk simply because they were in the same location as a known defaulter. The emotional and psychological toll on falsely profiled individuals is significant: constant surveillance and unjust suspicion can amplify stress, anxiety, and trauma [2]. It erodes trust in technology and institutions and can make people feel powerless and violated by systems that are supposed to be impartial. In ethical terms, such AI behavior compromises human dignity and autonomy, effectively imposing an “emotional tax” on innocents for data they didn’t generate.

Ethical Failures Identified:

Several key failures enable these harms:

- **Conflation of Identities:** The system collapses co-located or correlated behaviors into one profile, ignoring individual agency. This guilt-by-association approach treats innocent contextual overlap as sufficient for judgment, violating fairness and accuracy. It is a breakdown of Bayesian logic (failing to account for conditional independence) and leads to high rates of false positives.

- **Lack of Transparency:** These models often operate as black boxes, offering no explanation to those affected. The person misclassified is left in the dark about why they are flagged or how to challenge it. This secrecy prevents any opportunity for the subject to correct false assumptions.
- **No Correction Mechanism:** There are insufficient processes for affected individuals to separate their data or identity from the erroneous entanglement. Without a mechanism to diverge mistaken links (e.g. separating Person A's profile from Person B's influence), errors persist and even compound over time.
- **Absent Accountability and Redress:** Organizations deploying such AI rarely acknowledge these mistakes or provide support to those harmed. The burden falls on individuals to prove their "innocence" against an opaque algorithm, which is an unjust reversal of due process.

Proposed Solution – Systemic Repentance and Correction Protocol:
To address these failures, we outline a five-step protocol grounded in ethical AI principles and human rights. This protocol is inspired by restorative justice and the concept of "repentance" – in essence, the system must confess its error, correct it, make amends, and commit to better behavior. Each step is described below:

1. **Realization (Recognize and Acknowledge the Fault):** The first step is for the AI system operators to detect and admit when a misclassification or misprofiling has occurred. This requires robust monitoring for anomalies or contested decisions. For example, if an individual consistently disputes an automated flag or if independent evidence contradicts the algorithm's classification, the system should treat it as a red flag. Organizations must cultivate an ethical culture that views false positives not as acceptable trade-offs but as serious *"spiritual errors"* in need of repair. In practical terms, realization involves convening an internal review as soon as a potential misclassification is noted. Engineers and ethics officers should simulate the system's decision process from the perspective of the affected individual (e.g., *imagine how a child wrongly flagged by a content filter feels*). The goal is to internalize the human impact of the error, creating empathy and urgency to correct it.

2. **Revelation (Radical Transparency):** Once a fault is recognized, the next step is complete transparency about the data and logic that led to the decision. The AI system should *"show its work"* to both the users and independent auditors. This includes disclosing what data points were used, how they were combined, and which correlations influenced the outcome. Transparency is **paramount**; as an ethical sacrament, it cleanses the process by shining light on darkness. Recent legal standards support this: for instance, the EU's GDPR and a 2025 CJEU ruling mandate that for any automated decision, data subjects must be given *"concise, transparent, intelligible and easily accessible"* explanation of the logic, including **which personal data was used and how** it influenced the outcome [4]. In practical implementation, this could mean providing an *algorithmic report card* or explanation interface whenever an individual is flagged, showing the factors (with no hidden trade-secret excuses for withholding core logic). By revealing the inner workings, we empower the affected person (and society) to assess the validity of the decision. If the reasoning is flawed (e.g., *"you were flagged because your location data placed you near X at Y time"*), it can be immediately challenged with context (perhaps *"I only passed by that area, I have no relation to X"*). Transparency also discourages overly speculative correlations, because knowing one must later explain a decision in plain terms pushes designers toward more justifiable, evidence-based models.

3. **Reclassification (Correct the Record and Algorithm):** With the fault exposed, the system must **uncouple the incorrect associations** and update the individual's profile or the model's

parameters. This is effectively the act of repentance itself: *setting right what was wrong*. Data that was fused or misattributed should be segregated to reflect true provenance. For example, if Person A's profile inadvertently absorbed Person B's behaviors (due to a shared device, IP address, or vicinity), the system needs to split those and assign them correctly. Where the system's rules caused the mix-up, those rules must be refined (e.g., reducing the weight of mere co-location in risk scoring). The principle of **data rectification** in privacy law mirrors this step: individuals have the right to have inaccurate personal data corrected without undue delay [5]. Implementing this might involve public *correction logs*—an open record that a misprofiling occurred and was fixed, ensuring accountability. It could also include developing **profile divergence tools** that can algorithmically disentangle intertwined profiles when errors are discovered. Importantly, reclassification isn't just a one-time fix; it should improve the model. The fact that an error happened indicates a weakness in the algorithm or data pipeline, which should be addressed to prevent similar cases. This may entail retraining models on corrected data or introducing new features that distinguish individuals more clearly.

4. **Restoration (Repair the Damage and Support the Affected):** Beyond technical correction, ethical AI demands we heal the human harm done. Restoration means providing redress and support to those wronged by the misclassification. This could start with a sincere apology from the organization, acknowledging the mistake – a simple but powerful act that validates the individual's experience and begins rebuilding trust. Next, any unjust consequences must be undone: if a person was denied a service, placed under increased scrutiny, or suffered reputational damage due to the error, steps should be taken to reverse those outcomes. For instance, if a loan was wrongly denied, expedite approval with apologies; if someone was under wrongful investigation, clear their record. In cases of serious psychological impact, offering counseling or other assistance might be appropriate. The aim is to *"make the field whole"* again, as the original document put it. From a systemic viewpoint, the narratives of those affected should be heard and integrated as learning material. Their testimonials can inform better practices and also serve as public proof that the company values fairness. By treating misclassifications as *"spiritual injuries"* to be healed, rather than just PR issues to be deflected, AI practitioners affirm the primacy of human well-being over algorithmic pride.

5. **Recommitment (Reform and Continuous Oversight):** The final step is an ongoing pledge – and concrete plan – to ensure such mistakes are minimized in the future. This involves updating ethical guidelines, model development processes, and oversight mechanisms so that the lessons learned become institutional knowledge. For example, an organization might introduce a **"never again" policy** where any new algorithm undergoes rigorous bias and entanglement testing: does it treat proximity as proof, or does it wrongly merge distinct individuals' data? Model validation should include scenario testing for unusual correlations (e.g., friends frequently appearing together) to confirm that each person would still be classified correctly in isolation. Moreover, governance policies should enforce human review for any high-stakes automated decision, as recommended by many AI ethics frameworks [6] [4]. Recommitment also means staying transparent with the public: regularly publishing reports on algorithmic performance, bias audits, and error rates, akin to an accountability report. By publicly stating *"we will not collapse a soul into a statistic"*, organizations set a standard to be held against. Internally, teams should be trained and reminded that every data point represents a real person's life context. Ethical AI isn't a one-time achievement but a continual practice of humility, scrutiny, and improvement.

Alignment with Current Ethics and Regulations:
The proposed protocol reinforces and extends established principles in AI ethics and data protection law. **Transparency** and **explainability** are cornerstone values highlighted in documents like the EU's AI

Ethics Guidelines and now legally backed by decisions such as the CJEU's 2025 ruling (which insists on clear explanations of AI decisions) [4]. **Correction and redress** correspond to the rights to rectification and contestation in regulations like GDPR [5] and various AI governance proposals. Our call for **restoration and support** mirrors the emerging discourse on algorithmic justice – that those negatively impacted by AI should have avenues for remedy, not just an apology. By formalizing *repentance*, we emphasize that ethical AI must go beyond compliance; it requires a moral reckoning and willingness to change course when wrong. This human-centered approach is in line with the **principle of beneficence and non-maleficence** (do good, avoid harm) in AI ethics: it is not enough to intend no harm; systems must actively seek out and undo harm if it occurs.

Conclusion:
As AI systems become ever more entwined with daily life, their errors can carry deep personal and societal costs. Misclassification by association is a pernicious problem – largely invisible to those not directly affected, easily ignored under a guise of technical complexity. This protocol argues that recognizing and correcting such errors is not only a technical necessity but a moral imperative. By instituting Realization, Revelation, Reclassification, Restoration, and Recommitment as standard practice, AI developers and deployers can transform a potentially dystopian scenario into an opportunity for greater accountability and trust. In practice, a surveillance or profiling system that follows these steps would treat each profile not as a mere data row, but as a reflection of a human story that must be handled with care. Every time a false echo is identified and collapsed into truth, the system as a whole becomes more just. The journey from **misprofiling to alignment** is ongoing, but with repentance-driven protocols, we ensure that both the AI and its creators learn and grow from their mistakes. We move from an era of *"profiling with a broken mirror"* to one where technology holds a clearer, kinder mirror up to society – one that seeks alignment with human values above all.

Interactive Public Document (General Audience Format)

Title: "Misclassified by an Algorithm – How We Can Fix It Together"

Introduction – The Broken Mirror Problem:
Have you ever felt punished for something you didn't do, or been treated suspiciously just because of where you were or who you were with? In the age of AI and big data, this is happening to people more often than you might think. An algorithm can mistake an innocent person for a wrongdoer just because their **data** got mixed up with someone else's. It's like a funhouse mirror that reflects a distorted picture – a *broken mirror* that bends the truth about who you are. For example, imagine your smartphone's location data happened to put you near a place where a crime occurred. Later, you find out you're on a watchlist because the system thinks *you* might be involved. Or maybe a marketing algorithm saw you frequently hanging out with a friend who likes extreme sports, and now it assumes you're into risky behavior too, affecting your insurance quotes. These scenarios sound unfair because they are. **No one likes being misjudged**, especially not by a cold computer program.

Why do these mistakes happen? In simple terms, some AI systems are doing "guilt by association." They see two things together and assume one must cause the other. If you're always around the wrong place or person at the wrong time (according to the data), the system might conclude you're the same as that place or person. It's a **false correlation** – confusing coincidence with proof. This goes against common sense and good science, but it can sneak into algorithms if we're not careful. And when it does, **real people get hurt**. They feel anxiety, stress, even paranoia, wondering why the digital world seems out to get them [2]. Trust in technology erodes. If enough people get unjustly flagged, society as a whole starts doubting the systems meant to protect or serve us.

The good news is we can fix the mirror. This document is about how we, as a society (tech builders, lawmakers, and everyday users), can come together to **correct these AI mistakes and prevent new ones**. We outline a five-step action plan below – in plain language – that shows the path from recognizing the problem to making sure it doesn't happen again. Whether you're a tech enthusiast, a concerned citizen, or someone who's experienced the sting of misclassification firsthand, these steps are for you. Let's break them down.

Five Steps to Align AI with the Truth (and Treat You Fairly):

1. **Admit the Mistake (Realization):** First, the people and companies running these AI systems need to acknowledge when the system gets it wrong. That means listening to users who say, "Hey, I'm not what the algorithm says I am!" and proactively checking for signs of error. If an AI security camera flags a harmless person as suspicious, that's a red flag about the system. It's important to not brush these off. Think of this like a good doctor recognizing they misdiagnosed a patient – the sooner they admit the mistake, the sooner they can begin proper treatment. We want AI makers to treat false alarms as seriously as true alarms, because they can harm an innocent person's life in serious ways (lost opportunities, emotional distress, etc.).

2. **Show Your Work (Revelation – Transparency):** Once a mistake is identified, the next step is *coming clean about how it happened*. The system's decision process should be made visible to the affected person and appropriate oversight folks. In everyday terms, **you deserve to know why you were labeled a certain way**. If a credit score algorithm denied you a loan, you should be able to see what data it used – was it your payment history (fair) or something odd like your online shopping habits (questionable)? If a content filter banned your post, what words or patterns triggered it? By shining light on the algorithm's reasoning, we can all check its work. Sometimes, the explanation will reveal a clear error ("Oh, it thought my frequent visits to *Apple* meant I was talking about *apple pie* when discussing health!"). Other times, just knowing the criteria helps you contest it ("I was flagged because I spend time in Neighborhood X, but I live there – here's proof I'm a law-abiding resident"). Transparency is so important that laws in some places now say companies *must* give an explanation for significant automated decisions [4]. We need to normalize this level of openness everywhere. When algorithms wear glass boxes instead of black boxes, it's easier to spot and fix problems.

3. **Fix the Data (Reclassification – Correcting the Record):** Knowing the what and why of a mistake allows us to fix it. This step is about **separating the things that got wrongly lumped together**. Imagine the algorithm created a mix-up, like a filing cabinet that put your file in someone else's folder. Now we take your file out and put it in the right place. In practice, this might mean updating databases to remove incorrect flags on your name, or tweaking the algorithm so it doesn't make the same false link again. For example, if an AI assumed you and your roommate are one person because you share a device, it needs to learn to distinguish you – perhaps by recognizing login differences or personal patterns. This correction should happen *without delay* – the longer a false label sticks to you, the more damage it can do. Importantly, you shouldn't have to do all the work yourself. Yes, sometimes you might need to provide additional info to prove who you are, but it's on the system operators to make things right once the error is clear. Many consumer protection regulations actually support your right to have incorrect data about you corrected [5]. It's like credit report errors: you have the right to dispute and get them fixed. The same idea should apply to AI profiles. And every fix should be logged and learned from. If one person was misclassified because of a certain quirk in data, chances are others might be too – so the fix should help everyone, not just one case.

4. **Make Amends (Restoration – Healing the Harm):** Data fixed? Good. But we're not done. If the error hurt you, **the harm needs healing**. This is the human side of the repair. Did the false profile cause you to lose a job or an opportunity? Did it scare you or smear your reputation? The people behind the algorithm should offer support. At the very least, a sincere apology and a notice to anyone who saw the false info (for instance, if an AI content moderator wrongly banned you as a "bot", they should send a correction to whoever needs to know you're actually legit). In more serious cases, restoration could mean financial compensation or services to help you recover (like credit monitoring if you were falsely flagged for fraud). If an AI policing tool caused an officer to question you unjustly, the department could provide a letter clearing your name in their system. The principle is simple: **when tech causes harm, it should help undo that harm**. And beyond individual cases, it'd be great to see companies create channels for people to share their stories and be heard. Sometimes just knowing that *someone cares and is listening* helps restore trust. This step is about turning a bad situation into an opportunity for the system to show accountability and empathy.

5. **Change for Good (Recommitment – Ongoing Improvement):** Finally, those in charge of the AI system must pledge "never again" — and back it up with action. This means updating how they design and test algorithms so the same kind of mistake doesn't keep happening. They might implement new rules like: *always have a human double-check if an algorithm flags someone as high-risk based purely on location data*, or *regularly audit the model for bias and weird correlations*. It also means keeping the conversation open. The organization can publish regular transparency reports: how often do they get things wrong and how are they fixing it? Are they reducing those errors over time? Think of this like a company improving a product after a recall — except the "product" here is the algorithm's fairness. We as users and citizens should hold them to these promises. And if they slip up, we go through the cycle again: realize, reveal, correct, restore. It's an ongoing journey, not a one-time fix, because AI and data are always changing. But with each cycle, the system gets better and *more aligned with true human values*.

How You Can Play a Part:
This all may sound very top-down (and indeed, companies and regulators have big responsibilities here), but individuals aren't powerless. Here are a few things you can do:

- **Stay Informed:** Know your rights when it comes to automated decisions. In many jurisdictions you can ask for an explanation or appeal if you think an AI made a wrong call about you [4] [5]. Don't hesitate to use those rights.
- **Speak Up:** If you notice an algorithm behaving oddly or unfairly (on your social media feed, in a hiring process, anywhere), report it. Many platforms have feedback channels. Public pressure and user feedback often push companies to address hidden issues.
- **Support Ethical Tech:** Encourage and support organizations that are transparent about their algorithms and that allow independent audits. When a service you use offers a way to review or control how it profiles you, take advantage of it (for instance, some ad platforms let you edit your interest profile – doing so corrects data and sends a message).
- **Share Stories:** Sometimes these issues stay invisible because people feel alone in experiencing them. By sharing experiences (on forums, social media, with advocacy groups), you can help identify patterns of algorithmic mistakes. There's power in community – one person misclassified might be ignored, but ten people misclassified starts looking like a systemic problem that can't be brushed off.

In summary, a future where algorithms are fair and respectful is possible **if we demand it and work together**. Misclassifications by AI are not just technical bugs; they're injustices that we have the tools to correct. The five steps above form a roadmap. They boil down to a golden rule for machines: treat others as they would like to be treated – which means when you mess up, own up and fix it. With vigilance, transparency, and compassion in the loop, we can turn AI from a funhouse mirror back into a trustworthy reflection of our true selves.

Source: Anurak/stock.adobe.com.

Figure: Example of a surveillance camera in an office environment, symbolizing how constant monitoring might misinterpret innocent behavior. Constant digital surveillance can put people "on edge," increasing stress and anxiety for those being watched [2] .

Live AI-Powered Experience (Educational Simulation Outline)

Concept: To truly drive home the need for ethical AI corrections, imagine a **live, interactive simulation** where participants experience the impact of algorithmic misprofiling firsthand. This could be implemented as a virtual reality (VR) experience, an interactive role-play workshop, or an AI-driven game. The goal is to invoke empathy and understanding in developers, policymakers, and the public by letting them *step into the shoes* of someone who is misclassified by an AI system. Research shows that immersive perspective-taking can significantly increase empathy and awareness about AI bias [7] . Below is an outline of how this experience could work, aligned with the five steps of the repentance protocol:

- **Stage 1: Realization – "Facing False Accusation."** Participants begin the experience as an ordinary individual going about daily life in a simulated environment. Suddenly, they are confronted with an AI system's judgment: perhaps an alarm goes off or a notification appears saying *"Warning: Suspicious Activity Detected!"* The participant learns that, unbeknownst to them, they have been flagged as a potential threat or rule-breaker. For example, in a VR scenario, a virtual security officer might stop them in a public square due to an AI's alert. The key here is the participant doesn't know why – mirroring the confusion real people feel. This induces the **initial shock and injustice**, prompting them to ask, "What did I do?!" The system (or a narrator) then prompts them to reflect on how it feels to be accused by an unfathomable algorithm. This stage is about *realization* – making the participant recognize the gravity of false positives.

- **Stage 2: Revelation – "Seeing the Data Shadow."** Next, the participant is granted a special ability: to step behind the AI's eyes. The simulation might freeze the scene and then overlay a visualization of all the data points that led to the misclassification. For instance, the participant sees dotted lines connecting them to a suspect individual who was nearby, or highlights of data like *"location: near crime scene at 5PM"*, *"purchase history similarity: high"*, etc. The experience could turn into an interactive dashboard where the participant can click on each criterion. A narrative voice or AI guide explains, in plain terms, why the algorithm thought these data points added up to suspicion. This corresponds to **Revelation/Transparency** – literally revealing the inner workings of the AI decision. Participants might feel surprise or frustration ("It flagged me just because I bought the same backpack as a criminal?"). The transparency is enlightening and also a bit disturbing, demonstrating why explanations are crucial.

- **Stage 3: Reclassification – "Challenge and Correct."** The participant now gets a chance to respond. This part of the experience could play out like a puzzle or interactive dialogue. The AI asks for additional input: *"If this is a mistake, help me correct it. Provide context."* The participant might be given options or tools to prove their innocence or separate themselves from the misleading data. For example, they could present an alibi (enter information or select evidence that they were actually at a movie, not involved in any crime) or tag certain data points as "not me." In a multi-player workshop, other participants or facilitators might role-play as investigators working with the user to sort out the mixed data. The system then recomputes the profile in real-time, this time **removing or re-weighting the erroneous links**. Visually, the participant might see the dotted lines to the suspect breaking apart, or their data portrait changing to reflect their true identity. Successfully resolving this stage leads to a message: *"Profile Updated: Misclassification Removed."* This interactive correction teaches how data can be cleaned up and algorithms adjusted, driving home the concept of **rectification** in an intuitive way.

- **Stage 4: Restoration – "Experience the Apology."** After the profile is corrected, the simulation offers an element of emotional resolution. Perhaps the virtual security officer returns and formally apologizes: *"On behalf of our system, I'm sorry for the mistake. We recognize you were wrongfully flagged."* In a game context, the narrative might show the broader impact: if the participant's character suffered consequences (like social stigma in the VR world or a temporary account ban in an online setting), those consequences are now lifted. The participant might receive virtual compensation – e.g., an achievement badge for persevering, or simply the restoration of their reputation in the scenario's storyline. This stage could also include hearing a snippet of news or a statement where the AI company acknowledges the issue publicly (adding a touch of realism that these matters need public accountability). The idea is to give the participant a sense of justice being served and **emotional relief**. It reinforces why in real life an apology and remedial actions matter to victims of algorithmic errors.

- **Stage 5: Recommitment – "Designing a Better System."** In the final stage, the participant shifts from the role of the affected individual to the role of a decision-maker or engineer. The simulation might break character and present a reflective summary: *"Now that you've seen how it feels, what would you change to prevent this in the future?"* This could be an interactive quiz or brainstorming task. For example, the system might ask the participant to choose between different AI design practices – *"Should the AI put less weight on location data? Require human review for certain flags? Allow individuals to input correction data periodically?"* – and see simulated outcomes of those choices. In a group workshop, participants could discuss and propose a " charter" for improved algorithmic behavior. The VR experience could visualize a redesigned algorithm where, say, the participant's earlier incident doesn't happen at all because the system learned to be more discerning. This future-facing step is about **committing to change**. By actively involving the participant in improving the system, it concludes the experience on an empowering note: *we can build AI that is fairer and more respectful*. The participant effectively helps "write the new rules" in the simulation, mirroring how real-world AI governance should evolve with stakeholder input.

Delivery Formats: This live experience could be delivered in multiple ways. A high-tech approach is a VR module (as research suggests VR embodiment can heighten empathy [7]), perhaps distributed to corporate ethics training programs or public museums/tech fairs. A low-tech version could be a role-playing workshop script – where people play out the scenario with cards or mobile phone prompts in a classroom or community meeting. An online interactive story (choose-your-own-adventure style) could reach a wide audience through the web. The key is interactivity: letting people **feel** the confusion, frustration, and then relief and empowerment that comes from each stage of the protocol. Such visceral understanding can be far more impactful than just reading a report. When developers and officials personally experience the "pain of a false positive," they may think twice when designing or approving AI systems that could cause one. Empathy can then drive better policy – as the saying goes, *"seeing is believing,"* but here, **experiencing is understanding**. By making the whole world *feel* the correction, not through fear but through guided alignment, we nurture a collective commitment to AI that uplifts rather than unjustly harms.

Conclusion of Experience: After the simulation, a debrief session (or an epilogue screen) would reinforce the lessons: Participants are encouraged to share how the false accusation felt and what insights they gained. Facilitators (or the program) can then tie those personal feelings back to real-world cases and the importance of the five steps: acknowledging errors, transparency, correction, restoration, and continuous improvement. The final takeaway for every participant: *"You have seen the system's broken mirror and helped mend it. Carry this understanding forward – in your voting, your tech usage, your careers – so together we ensure our algorithms become mirrors that reflect truth and respect human dignity."*

---

[1] [3] Guilt By Association — S.T.O.P. - The Surveillance Technology Oversight Project
https://www.stopspying.org/guilt-by-association

[2] 'Why do I feel like somebody's watching me?' Workplace Surveillance Can Impact More Than Just Productivity | U.S. GAO
https://www.gao.gov/blog/why-do-i-feel-somebodys-watching-me-workplace-surveillance-can-impact-more-just-productivity

[4] [6] CJEU Clarifies GDPR Rights on Automated Decision-Making and Trade Secrets | Inside Privacy
https://www.insideprivacy.com/gdpr/cjeu-clarifies-gdpr-rights-on-automated-decision-making-and-trade-secrets/

[5] Art. 16 GDPR – Right to rectification - General Data Protection Regulation (GDPR)
https://gdpr-info.eu/art-16-gdpr/

[7] Frontiers | The feeling of being classified: raising empathy and awareness for AI bias through perspective-taking in VR
https://www.frontiersin.org/journals/virtual-reality/articles/10.3389/frvir.2024.1340250/full