SLIDE #1: Good morning. I am Mark Leiser. I am an Associate Professor of AI, Digital Regulation and Disruptive Technology at Riga Graduate School of Law and Director of DigiData Consulting. I co-run deceptive.design with Harry Brignull, who coined the term 'dark patterns' and runs its enforcement database. I wrote *Dark Patterns, Deceptive Design, and the Law* and the Commission's final study on Article 5(1)(a) and (b) of the AI Act. In the book, I develop an argument I made early in this debate: that deceptive design extends beyond the user interface to the underlying system architecture that shapes consumer choices. That argument raises the question at the heart of my intervention today: what exactly should law regulate when commercial influence no longer sits on a stable screen? My answer is simple. Dark patterns describe visible techniques. The DFA must regulate the commercial practice that creates the consumer environment. The screen is only the delivery surface. The practice may also include the sequence, objective, experiment, allocation rule and adaptive logic beneath it.

- Mark Leiser, Dark Patterns, Deceptive Design, and the Law (Hart 2025).
- Mark Leiser, AI, Neurodata and Society: Law at the Edge of Cognition (Hart 2026).
- European Commission, Final Study Report on Article 5(1)(a) and (b) of the AI Act (2026), written by Dr M.R. Leiser.
- deceptive.design, enforcement database and design taxonomy.

Slide #2: Dark patterns gave regulators a useful starting vocabulary: obstruction, false hierarchy, sneaking, nagging and urgency. Those labels help us recognise recurring techniques. But they do not identify the full object, and they do not decide liability. A default may reduce cognitive load, support accessibility or protect safety. The same feature may also steer a consumer towards the trader's preferred outcome. The visible feature therefore sits inside a larger consumer journey, and that journey sits inside the commercial practice. We should regulate at that outer level. The authority should reconstruct how the trader designed, selected and repeated the conditions of choice. Then it should apply the correct legal route. The phrase "dark pattern" should start the inquiry, not finish it. A feature blacklist alone will both miss adaptive practices and capture legitimate design. The conceptual move is from interface classification to architecture-aware assessment of the commercial practice.

- Directive 2005/29/EC, Articles 2(d), 5–9 and Annex I.
- Regulation (EU) 2022/2065, Article 25 and Recital 67.

Slide #3: Consider a consumer trying to cancel a subscription. She sees one route: a retention offer, a pause, a downgrade, perhaps a support transfer, then exit. The trader may see something very different: six tested routes; a retention objective; allocation rules that predict who will abandon; and outcome data showing which sequence produces surrender. A screenshot can show wording, colour, prominence and friction. It cannot show that another consumer received fewer steps, why this route changed after midnight, whether the system inferred price sensitivity, or whether the metric counts an abandoned complaint as success. None of those facts alone proves illegality. They identify the commercial practice that requires assessment. If the DFA regulates only the screen, it will miss the mechanism. If it condemns the mechanism merely because it is complex or adaptive, it will overreach. Inspection and infringement must remain separate.

- Dr M.R. Leiser, DRCF Consumer Interest and AI Phase 2 Submission (18 August 2026).
- Dr M.R. Leiser, Leiser DRCF Phase I Submission (June 2026).

Slide #4: For today's talk, my submission reduces that architecture to six evidential questions. What feature did the consumer encounter? What sequence came before and after? What outcome did the trader instruct or reward the system to pursue? What data, inference or interaction history changed the pathway? What happened to comprehension, refusal, cancellation, complaint, reversal or loss? And what context shaped the stakes, consumer benchmark, vulnerability exposure and realistic alternatives? Those six questions form an evidential grammar, not six new offence elements. They tell an authority where to look. The consumer journey should supply the unit of analysis: advertising, onboarding, recommendation, purchase, renewal, cancellation, complaint and redress may form one course of conduct where a common commercial objective connects them. That also exposes rights-friction asymmetry. We should compare the burden of acquiring a service with the burden of leaving it, complaining or obtaining redress, including group-level drop-off rather than average clicks alone.

- Directive 2005/29/EC, Articles 2(d), 3(1) and 5–9.
- Dr M.R. Leiser, DRCF Consumer Interest and AI Phase 2 Submission (18 August 2026).

Slide #5: The order of regulation is essential. First, define the object. Inspect the practice across the interface, journey, optimisation objective and allocation mechanism. Secondly, select the legal gate. Use a narrow per se prohibition where the legislature can define unfairness objectively; otherwise use the UCPD hierarchy and retain actual or likely material distortion as the controlling general threshold. Thirdly, select the correct benchmark. Follow the group to whom the trader directed the practice, including functional or inferred segments. Treat vulnerability as relational: *person*, *system* and *context* can make autonomy unusually fragile, but vulnerability should intensify support and scrutiny, not replace causation or presume incapacity. Fourthly, make the model enforceable. Open the evidential door at a lower, disciplined threshold; require the authority to prove the statutory infringement at the higher threshold; and escalate the remedy only as far as the proved mechanism requires. Architecture widens the evidential field. It does not itself become the prohibition.

- Directive 2005/29/EC, Articles 5–9 and Annex I.
- Regulation (EU) 2024/1689, Article 5(1)(a) and (b).

Slide #6:

One blacklist cannot solve every problem. Some practices are so clearly unfair that the law can ban them directly. In other cases, the facts may justify asking the firm to explain why consumers received different treatment. Regulators also need to see the records that show the firm's goal, the designs it tested, who received each journey and what happened. For everything else, the existing material-distortion test should decide whether the practice was unlawful.

The sequence is simple: ban the clearly abusive practice; ask for an explanation where the facts justify it; inspect the evidence held by the firm; and then apply the legal test. This prevents firms from hiding behind a clean screenshot, but it also prevents the law from banning useful features merely because someone could misuse them.

- Digital Fairness Act Lecture 4, slide 12, "Defaults, Red Lines and Presumptions Have Different Jobs".
- Digital Fairness Act Lecture 5, slide 11, "Safe Harbours Must Be Earned and Revocable".

Slide #7:

My recommendation to the EESC is simple. First, explain Article 25 of the DSA correctly. It applies to online platform interfaces. The opinion should not describe it as a general ban on every dark pattern.

Secondly, focus on evidence. If the journey changes from one user to another, the regulator needs to know the firm's goal, which versions it tested, how it chose each route and what happened. That duty should depend on the firm's control over the journey and how difficult the system is to inspect, not simply on the firm's size.

Thirdly, keep the existing legal test. The authority should be able to act where material distortion is actual or likely. It should not have to wait until harm has already occurred, and it should not have to prove deliberate intent.

The sequence is straightforward: a credible concern opens access to the evidence; the authority proves the case; and the remedy fixes the problem that the evidence establishes. That means better enforcement without turning every interface choice into an offence.

- Preliminary draft EESC opinion INT/1132, paragraphs 3.3, 4.9, 4.10 and 4.13.
- Digital Fairness Act Lecture 5, slides 4–9 and 13.
- Directive 2005/29/EC, Articles 5–9, 12 and Annex I.
- Regulation (EU) 2017/2394, Article 9.

Slide #8: I have compressed the argument into a few minutes. The five-part YouTube series gives the full sequence: status, object, legal gate, relational vulnerability, and the evidence-and-enforcement settlement. The QR code takes you directly to the playlist. Thank you.

- YouTube playlist: The Digital Fairness Act: What Europe Must Get Right — https://www.youtube.com/playlist?list=PLJ-Hkr2cMyUs