

HUMAN RIGHTS & DATA INTELLIGENCE

NAVIGATING THE INTERSECTION OF FUNDAMENTAL RIGHTS AND DATA LAW

WEBINAR | 20 July 2026

David Mitchell

Sam Fowles

Nyasha Weinberg

39 Essex Chambers

WHAT WE WILL COVER

Surveillance, biometric AI, algorithmic bias, GDPR compensation and generative AI are no longer niche concerns: they arise in public law, employment, health and social care, national security and commercial disputes alike. Case law current to May 2026.

Part 1 | Sam Fowles – Human rights and Live Facial Recognition

- From **Bridges** and **Big Brother Watch** to **Thompson & Carlo** [2026] EWHC 915 (Admin)

Part 2 | Nyasha Weinberg – GDPR compensation and generative AI

- The CJEU on pseudonymisation (**EDPS v SRB**) and abusive access requests; web scraping, agentic AI. Lessons from **Ayinde** AI, confidentiality and legal professional privilege

Part 3 | David Mitchell – GDPR compensation and generative AI

- The **Special Purposes Exemption**, the legal test for **consent** under GDPR, and the evolving DSAR landscape.

Closing – Key human rights challenges of AI; Q&A

WHY THIS MATTERS NOW

Data intelligence is now everyday legal practice

- Biometric surveillance, automated decision-making and generative AI are embedded in policing, welfare, health, employment and commerce
- Claims increasingly combine human rights, data protection, equality and public law grounds

The case law is moving fast

- **Live facial recognition:** from **Bridges** (2020) to **Thompson & Carlo** (April 2026) — and a Court of Appeal round to come
- **CJEU:** pseudonymisation is not always personal data (**EDPS v SRB**, Sept 2025); abusive/excessive data subject requests require proof of abusive intent (C-416/23)
- **Generative AI:** EDPB guidelines on web scraping (July 2026); privilege waived by uploading to open-source AI tools (**UK v SSHD (Hamid)** [2026] UKUT 81 (IAC))
- **AI in litigation itself:** fake citations and the Hamid jurisdiction (**Ayinde**, June 2025)

What solicitors need

- The cases that matter, the direction of travel, and practical guardrails for clients — and for your own use of AI

HUMAN RIGHTS AND LIVE FACIAL RECOGNITION

Sam Fowles

What LFR does

- Real-time capture of faces in public, converted to biometric templates and matched against police watchlists – a digital identity check without consent

Rights engaged

- **Article 8 ECHR** – biometric data is akin to DNA/fingerprints; capture and processing interfere with private life
- **Articles 10 & 11** – chilling effect on expression and assembly, especially at protests
- **Non-discrimination** – misidentification risk skews by race and sex; Public Sector Equality Duty

The legal framework – or its absence

- No dedicated statute: common law policing powers + Data Protection Act 2018 Part 3 + College of Policing APP (2022) + force-level policies
- The recurring question: is the interference “in accordance with the law” and proportionate?

THE FOUNDATIONS: BRIDGES AND BIG BROTHER WATCH

Sam Fowles

R (Bridges) v Chief Constable of South Wales Police [2020] EWCA Civ 1058

- First test case on police LFR — Court of Appeal held the deployments **unlawful**
- Article 8: “too broad a discretion” — no clear criteria on **who** goes on a watchlist or **where** LFR is deployed, so not “in accordance with the law”
- DPIA deficient; PSED breached — the force never properly investigated the risk of race and sex bias in the algorithm
- But LFR was not held inherently unlawful — the defects were in the safeguards, not the technology

Big Brother Watch v UK (ECtHR, Grand Chamber, 2021)

- UK bulk interception regime violated Articles 8 and 10
- Requires **end-to-end safeguards**: necessity and proportionality assessed at each stage, independent authorisation, oversight and ex post review
- The Strasbourg blueprint against which mass surveillance technologies — including biometrics — now fall to be tested

THOMPSON & CARLO V MET POLICE COMMISSIONER

Sam Fowles

R (Thompson & Carlo) v Commissioner of Police of the Metropolis [2026] EWHC 915 (Admin) – 21 April 2026

The facts

- Feb 2024: Shaun Thompson misidentified by Met LFR at London Bridge (matched to his own brother) – detained ~30 minutes, threatened with arrest despite producing ID; later received a compensation payment
- Second claimant Silkie Carlo (Big Brother Watch): LFR deters her attendance at protests

The challenge and the ruling

- Grounds: the Met's LFR policy confers too broad a discretion (watchlists/locations) – Articles 8, 10 and 11
- **Dismissed on all grounds:** policy contains “clear, interlocking and cumulative constraints”; the Bridges defects are cured by the Met's 2024 policy
- Articles 10/11 engaged at protests, but the policy's express duty to assess chilling effects is a real safeguard

Why it is not the last word

- A narrow, policy-level review – no PSED ground; hypotheticals refused; **appeal to the Court of Appeal pending**

LFR: WHERE NEXT?

Sam Fowles

Rapid expansion, thin legal foundations

- Jan 2026 policing White Paper: £26m national facial recognition system; £11.6m LFR expansion; vans from 10 to 50 across England and Wales
- May 2026: LFR deployed at a London protest and the FA Cup final – tens of thousands of faces scanned
- Still no statutory framework – police policy fills the gap; the Biometrics and Surveillance Camera Commissioner warns of a “patchwork of laws”
- EHRC considers the Met’s use unlawful; Home Office biometrics consultation closed Feb 2026 – legislation likely to follow Thompson & Carlo’s framing

Private-sector LFR

- Retail deployments (Facewatch and others) raise parallel UK GDPR issues: lawful basis, accuracy, watchlist fairness, no meaningful redress

Advising clients

- Challenge specific deployments and watchlist inclusion; misidentification claims sound in damages (see Thompson); DPIA and PSED compliance remain the pressure points

KEY HUMAN RIGHTS CHALLENGES OF AI

- **Privacy:** constant tracking and opaque data use create a structural power imbalance — companies know users' vulnerabilities; users don't know how their data is used
- **Discrimination:** facial recognition and language models have shown prejudice against racial and ethnic minorities — false arrests, marginalisation of the digitally excluded and disabled
- **Expression and information:** AI moderation over-suppresses lawful speech; bots, addictive design and echo chambers distort choice and democratic participation
- **Accountability and remedy:** secretive algorithms leave individuals unable to understand or challenge decisions — undermining the rights to be heard and to an effective remedy
- **Dignity and societal harm:** surveillance erodes autonomy and self-determination; harms are often invisible individually and visible only in the aggregate

The through-line

- Human rights considerations must run through the **entire AI lifecycle** — design to deployment — including human rights impact assessments

GENERATIVE AI MEETS THE GDPR

Nyasha Weinberg

Era one – generative AI (2022–): the questions still open

- Lawful basis for web scraping and training; special category data inevitably in the corpus; how to erase data from a trained model
- EDPB ChatGPT taskforce report (May 2024) remains “preliminary views”; the Garante’s OpenAI fine (Dec 2024) was overturned – most investigations still open

Era two – agentic AI (2025–): new problems on top

- **Controllership in agent chains:** one task, several sub-calls, several GDPR roles – you cannot outsource controllership; if you don’t vet the chain, the chain decides your role for you
- **Memory:** compartmentalise; retention limits; pseudonymise prompts and outputs before long-term storage; filter sensitive inferences; make memory subject-access ready
- **Security:** prompt injection, memory/RAG poisoning, silent data exfiltration – attack vectors regulators have specifically catalogued
- DPAs converging: Spanish AEPD “rule of 2” for agent risk; Dutch DPA (Feb 2026) – the deployer remains fully accountable

GDPR COMPENSATION: THE STATE OF PLAY

Nyasha Weinberg

Article 82 – the CJEU’s framework

- Three conditions: infringement + material or non-material damage + causal link – infringement alone is **not** enough (Österreichische Post, C-300/21)
- No seriousness threshold, but damage must be **actual and certain**, not hypothetical
- “Negative feelings” can qualify – but concrete evidence is required, and the seriousness of the controller’s fault does not increase quantum (Quirin Privatbank, C-655/23)
- Loss of control and fear of misuse can constitute damage – fertile ground after breaches and scraping incidents

Abusive and excessive requests

- C-416/23 (Österreichische Datenschutzbehörde): 77 complaints in 20 months – volume alone cannot make requests “manifestly excessive”; **abusive intent must be established** on the circumstances
- AG in Brillen Rottler (C-526/24): a first access request can be refused as excessive only in **exceptional circumstances** – strict criteria, controller bears the burden
- Practical: DSARs deployed tactically in disputes remain hard to resist; document any abuse case carefully

PSEUDONYMISATION: EDPS V SRB (C-413/23 P)

Nyasha Weinberg

CJEU, 4 September 2025 — the year's most consequential ruling on "personal data"

Background

- Banco Popular resolution: SRB shared pseudonymised stakeholder comments with Deloitte (codes only, no key) — data subjects never told

What the Court held

- **Opinions are inherently personal data** of their author — no separate analysis of content, purpose or effect needed
- Pseudonymised data is **not personal data in all cases and for every person**: identifiability is contextual — assessed from the recipient's perspective, asking whether re-identification is reasonably likely
- But transparency duties bite **at collection, from the controller's viewpoint**

Why it matters

- Data sharing, AI training sets, SARs and international transfers all affected — pseudonymisation is a genuine safeguard but never a silver bullet; tension with draft EDPB guidance still to be resolved

DEPLOYING GENERATIVE AI LAWFULLY

Nyasha Weinberg

Same principles, new technology

- GDPR obligations apply to generative AI procurement exactly as to any other processing (see e.g. Microsoft, GDPR and Generative AI: A Guide for the Public Sector) – the risk-assessment discipline does not change

The workstreams to interrogate

- Transparency to data subjects; handling of data subject rights across prompts, outputs and logs
- Controller/processor allocation and processor obligations in the contract stack
- Technical and organisational security measures; **DPIAs before deployment**; international transfer mapping
- Confirm the supplier's data protection addendum and privacy commitments extend to its AI services

For advisers

- Map where prompts and outputs go; check training-use carve-outs; document the assessment – regulators' first ask will be your DPIA and LIA paperwork

AI IN THE COURTS (1): WHY IT MATTERS

Nyasha Weinberg

The shift

- Pre-2022: AI as back-office assistance — document review, TAR, contract analytics
- Post-2022: public LLMs produce apparently authoritative pleadings, letters before action and submissions — front-facing legal communication

Why the system is exposed

- Courts depend on accuracy, traceability and accountability — lawyers are the filter; when the filter fails, judicial time is wasted, opponents incur cost, public confidence erodes
- Pre-action correspondence is the flashpoint: high-volume, formulaic, produced under cost and time pressure — ideal conditions for substitution rather than assistance

The emerging judicial position

- AI use is not prohibited: courts distinguish **assistive use** (a tool under supervision) from **substitutive drafting** (replacing legal judgment)
- Three risk fronts: regulatory (duties are personal and non-delegable), procedural (strike out, sanctions, costs) and reputational — accountability is tightening, not relaxing

AI IN THE COURTS (2): DETECTING AI-GENERATED MATERIAL

Nyasha Weinberg

Linguistic indicators

- Over-formalised, generic legal language — no specific obligation, breach or date
- Fluent but non-specific reasoning: confident conclusions with no legal tests or factual steps
- Boilerplate reused across unrelated fact patterns; rhetorical certainty (“incontrovertible”) unsupported by pleaded evidence

Substantive red flags

- **Hallucinations:** authorities that “sound right” but cannot be located; invented quotations and paragraph references
- **Stale training data:** repealed CPR provisions, wrong time limits, missed practice direction changes
- **Blended jurisdictions:** English, EU and US standards mixed within a single legal test

AI-generated evidence

- Text, images, audio and video now near-indistinguishable from the genuine article — forgery becomes systemic risk, and authentic evidence gets challenged as fake (the “liar’s dividend”); expect satellite authenticity disputes and heavy reliance on experts

AI IN THE COURTS (3): RESPONDING AND ADVISING

Nyasha Weinberg

Responding to AI-tainted pleadings

- Attack substance, not technology — you need only identify legal defects, not prove AI use; avoid accusations
- Call out unlocatable authorities precisely; use fake cases and mistaken grounds to dismantle the argument
- Procedural levers: requests for further particulars, strike out, wasted costs, sanctions, totally-without-merit orders — neutral highlighting of errors often prompts the court to act itself

Advising clients on their own AI use

- AI can assist drafting but cannot replace legal judgment — a lawyer must verify every output
- Never enter confidential or personal data into public models; use approved tools; document safeguards and review processes

The GDPR dimension

- AI use is processing: identify a lawful basis, minimise, consider DPIAs for systemic use — data breaches may arise before any litigation risk does

AYINDE V HARINGEY; AL-HAROON V QNB [2025] EWHC 1383 (ADMIN)

Divisional Court (Dame Victoria Sharp P and Johnson J), 6 June 2025 – the leading Hamid judgment on AI

The two cases

- **Ayinde:** pupil barrister's JR grounds cited five non-existent cases and misstated s.188(3) Housing Act 1996; errors dismissed as “cosmetic” – wasted costs of £2,000 each against counsel and the law centre, and referrals to the BSB and SRA
- **Al-Haroun:** 45 citations – 18 wholly fictitious; the solicitor had relied on his client's AI-assisted research: a “lamentable failure” (one fake authority was even attributed to the judge hearing the case)

What the Court laid down

- Free generative AI tools “are not capable of conducting reliable legal research” – anyone using them must check outputs against authoritative sources
- The court's toolkit: admonishment, costs and wasted costs, strike out, regulatory referral, contempt, police referral – admonishment alone will rarely suffice
- Leadership accountability: heads of chambers and managing partners must take practical, effective measures – and can expect the court to ask whether they have

UK V SSHD (AI HALLUCINATIONS; SUPERVISION; HAMID)

[2026] UKUT 81 (IAC) – Upper Tribunal applies Ayinde, and goes further

- Two immigration cases with fake citations – one probably from inadvertent use of Google’s “AI Mode”: hallucination risk is not confined to chatbots
- **Supervision:** delegation does not delegate responsibility – a supervisor who fails to check a junior’s work is likely **more** culpable than a lawyer failing to check their own; SRA referral made
- **New statements of truth:** the UT judicial review claim form now requires confirmation that every cited authority (a) exists, (b) can be located by its citation, and (c) supports the proposition – sign it over false authorities and expect regulatory referral

AI, confidentiality and privilege

- Uploading confidential documents to an **open-source AI tool (e.g. ChatGPT)** places them “on the internet in the public domain” – breaching confidentiality, **waiving legal professional privilege**, and warranting referral to the regulator and the ICO
- Closed tools operating within a secure network (e.g. Copilot) distinguished – but store prompts and outputs securely and restrict access (Norton Rose Fulbright)
- Direction of travel is international: US v Heppner (SDNY, Feb 2026) – no privilege in a client’s exchanges with a public consumer AI tool

LAURENCE WESTGAP V MILL MEDIA – THE “SPECIAL PURPOSES EXEMPTION”

Personal information may be exempt from the right of access if processed for:

- journalistic purposes;
- academic purposes;
- artistic purposes; or
- literary purposes. (DPA 2018, schedule 2, paragraph 14)

Exemption applies based on controller's reasonable belief publication in public interest (taking into account “the special importance of the public interest in the freedom of expression and information”) and that compliance with a DSAR would be incompatible with the special purpose.

VINCE V ASSOCIATED NEWSPAPERS [2026] EWCA CIV 899

Labour repays £100,000 to 'sex harassment' donor

By **David Churchill**
Chief Political Correspondent

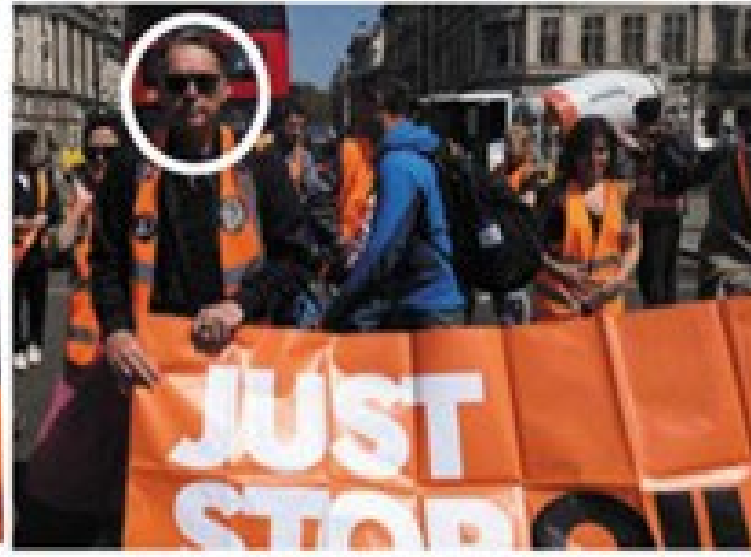
SIR Keir Starmer was left embarrassed yesterday after repaying a £100,000 donation to a high-flying City financier accused of sex harassment.

The Labour leader was forced into a humiliating climbdown after being accused of 'hypocrisy' for accepting the cash despite the allegations against Davide Serra.

Mr Serra, the boss of a multi-billion pound asset management firm in London, made four £25,000 donations to Labour during the first quarter of this year, it emerged in official figures released yesterday.

And Labour faced further embarrassment yesterday when businessman Dale Vince, who has donated £1.5million to the party, joined an eco-protest in London with Just Stop Oil, the group he is helping to bankroll.

The party pocketed Mr Serra's money despite accusations that



Road blockers: Dale Vince in London yesterday, and circled as he holds up traffic with Just Stop Oil

the 52-year-old married chief executive made 'wholly inappropriate' comments on the size of a female colleague's breasts.

A tribunal also heard he told cli-

ents that Jolanda Niccolini, his now former head of business development and investor relations, would do anything for them - 'including prostitute herself'. Mr Serra's firm

was ordered to pay £32,000 in compensation by a tribunal judge last month after Ms Niccolini successfully sued for sex harassment and victimisation. Labour has decided

to repay the £100,000 donation after the Daily Mail highlighted the case. It is understood it did not know about it before being alerted to it by this newspaper.

Earlier, Tory MP Craig Mackinlay said: 'If [Sir Keir] had principles he would hand the money back, otherwise it's hypocrisy.'

In central London yesterday, Mr Vince joined J80 activists who were blocking traffic around Parliament and Trafalgar Square.

Some suspect he may have influenced Sir Keir's pledge to block new North Sea oil and gas exploration if he wins the next election.

Mr Vince said: 'I'm here to support the incredibly brave people of Just Stop Oil. I can't imagine it will make much difference to Keir Starmer, he's his own man and so am I.'

Tory Party deputy chairman Nickie Aiken said: 'As if it wasn't already clear enough, Labour's big bankrollers and policy paymasters are the eco-fanatics themselves.'

“THIS CLAIM IS NOVEL IN THAT NO SUCH CLAIM HAS EVER, TO THE PARTIES' KNOWLEDGE, SUCCEEDED BEFORE.” [54]

Libel claim struck out (it is a basic principle of the law of defamation that the meaning of an article is based on the article as a whole, not just a headline).

Article 5 claim also struck out and summary judgment for D: *“Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')”*

CA reinstates Article 5 claim and enters summary judgment for C: s.12 HRA “relevant privacy code” includes IPSO Editors' Code of Practice which makes clear that newspapers must “take care not to publish ... misleading ... information or images, including headlines not supported by the text”.

OTHER RECENT CASES OF INTEREST

RTM v Bonne Terre Ltd [2026] EWCA Civ 488: consent under data protection law and the Privacy and Electronic Communications (EC Directive) Regulations 2003 is a purely objective concept.

Good Law Project Ltd v Reform Party Ltd [2026] EWHC 1458 (KB) (refusal to strike out or enter reverse summary judgment on representative claim). GLP, a not-for-profit organisation, had a reasonable basis for arguing at trial that it satisfied the conditions in s.187(3) and s.187(4) DPA 2018 to act as a representative body under Article 80 UK GDPR.

WRAP UP

Three takeaways

- **LFR:** lawful in principle after Thompson & Carlo — but the battleground moves to the Court of Appeal, specific deployments and the coming statutory framework
- **GDPR:** compensation doctrine is settling (actual, certain damage; no fault threshold), while EDPS v SRB and the scraping guidelines redraw the perimeter of “personal data” for the AI age
- **AI in practice:** verify everything, supervise everyone, and keep confidential material out of open tools — privilege, confidentiality and your practising certificate are all at stake

Questions & discussion

- David Mitchell • Nyasha Weinberg • Sam Fowles
- clerks@39essex.com | 39essex.com

39 Essex Chambers LLP is a governance and holding entity and a limited liability partnership registered in England and Wales (registered number 0C360005) with its registered office at 81 Chancery Lane, London WC2A 1DD. 39 Essex Chambers' members provide legal and advocacy services as independent, self-employed barristers and no entity connected with 39 Essex Chambers provides any legal services. 39 Essex Chambers (Services) Limited manages the administrative, operational and support functions of Chambers and is a company incorporated in England and Wales (company number 7385894) with its registered office at 81 Chancery Lane, London WC2A 1DD.

39essex.com

BARRISTERS • ARBITRATORS • MEDIATORS

LONDON • SINGAPORE • DUBAI • KUALA LUMPUR

