AI conquers the human eye: can technology overhaul disclosure in complex criminal cases?

Published on 20 March 2025, 'Disclosure in the Digital Age', Part one of Jonathan Fisher KC's Independent Review of Disclosure and Fraud Offences (the '**Review**'), properly and unsurprisingly accepts defeat on behalf of the human eye when it comes to disclosure in the Digital Age. At a time when even children own devices containing hundreds of gigabytes of data, it is no longer realistic, practical or desirable for investigating officers to sit in windowless rooms sifting through the material held on the devices of directors and bankers, never mind the material on the servers of the companies they work for.

There has never been a perfect disclosure regime. Those that held up in theory, all too frequently fell over in practice. One of the most fascinating and enjoyable sections of the Review, certainly for history and jurisprudence wonks, is the first – A History of Disclosure and the Right to a Fair Trial. It is striking that each overhaul and each review, from the first time a disclosure obligation was placed on the Crown in 1946 to the Review itself, was triggered by one or more miscarriages of justice. Systems which practitioners knew were failing almost daily in many different ways were tolerated until the worst effects materialised. Each new system, review and legislation was targeted at what was perceived to be the predominant problem of the day. By way of example, the fact that cases were brought and conducted by the Police themselves may seem incredible now in 2025, but it was only the Prosecution of Offences Act 1985 that changed that. It is perhaps not always easy to remember that the Crown Prosecution Service was created by that Act in order to ensure cases were prosecuted properly and fairly.

The trigger for this review was the collapse of the SFO prosecution of former directors of Serco Geografix Limited and the report on the disclosure failings by Brian Altman KC, published in July 2022. However, the inexorable rise in the prevalence and volume of digital material was, and is, causing such consistent and fundamental disclosure issues in criminal cases that a new approach was clearly required.

The Review makes 45 recommendations which include an updated Code of Practice and consolidated CPIA guidance, improved and more consistent training, more pre-charge engagement with prosecution counsel to consider reasonable lines of enquiry and an Intensive Disclosure Protocol to better manage disclosure from PTPH onwards in the most complex cases. All well considered and pragmatic recommendations to address weaknesses in the current regime, if not exactly reinventing the wheel.

There is real innovation in the Review however and the clue is perhaps in the title. Although Jonathan Fisher KC makes it plain that the Review covers the full spectrum of criminal cases[1] and that not all of the problems identified with disclosure are caused by the increased volume in digital material[2], it is clear that the Digital Age is not well served by an analogue disclosure regime. It is high time that the criminal justice system fought technology with technology. Change is happening, but far too slowly.

[1] The Review at paragraph 422 page 131
[2] Ibid at paragraph 418 page 130

Adopting the technological solutions considered, and recommendations made, in chapter 4.1 will undoubtedly accelerate that change[3].

The Review recommends establishing a Criminal Justice Digital Working Group to co-ordinate the assessment of existing technological tools which currently manage disclosure and evidence[4]. All aspects would be evaluated including accuracy, security and value for money, as well as skills, training and the requirement for regular reviews of that training.

The increased use of technology in the disclosure processes would be permitted by amendments to the CPIA Code of Practice recommended by the Review. These would include a new 'reviewing material' section to make it clear that technology can be used to identify relevant material[5] and amending s6 of the Code to allow for the use of technology in creating schedules[6] and the appropriate use of 'metadata schedules'[7].

Most, if not all, of these aims would be better achieved with some consistency in the use of such tools across the criminal justice system. There are issues of funding and procurement, as the Review acknowledges, but this is surely a time to invest in order to reap the benefits later. Can there be any justification for different agencies negotiating separately with the same provider of a material management tool, as the Review uncovered?[8] Or for different agencies utilising different tools?

Earlier this year the SFO piloted Technology Assisted Review (TAR) and reports that it reviewed documents for disclosure up to 40% faster. In the Foreword to the 2025-2026 Business Plan Nick Ephgrave says that the case management system will now be delivered and will further streamline their casework[9]. Such tools have been used by law enforcement agencies overseas and by white collar defence firms in the UK for some time, but they are expensive. If the SFO has one that has been tested and works surely it would be better value for money if other agencies look at the same tool?

The Review recommends that law enforcement agencies consider a central technological procurement unit[10]. That no such unit already exists must be astonishing to anybody unfamiliar with the criminal justice system. This recommendation must be adopted and implemented urgently.

The Review also recommends a cross-agency protocol to cover the ethical and appropriate use of AI in the disclosure process[11]. This is imperative and would break with all traditions of the criminal justice system by acting early, rather than playing catch up. The use of AI is currently limited and has already met with some difficulties. The SFO had to notify all defendants potentially affected by an encoding error on

[3] Ibid at page 130
[4] Ibid at paragraph 428-9 page 132-3
[5] Ibid at page 139
[6] Ibid at paragraph 451 page 140
[7] Ibid at paragraphs 456-7 page 142
[8] Ibid at paragraph 420 page 131
[9] https://assets.publishing.service.gov.uk/media/67ee4e86199d1cd55b48c6e8/SFO_2025-26__Business_Plan.pdf
[10] The Review at paragraph 433 page 134-5
[11] Ibid at paragraph 430-2 page 134

Axcelerate, an issue that took months to fix[12]. So now is the time to establish these protocols, not in 5 or 10 years' time when its use is commonplace but haphazard.

Few developments, whether in the legal system or elsewhere, provoke such extreme reactions as AI. It seems to excite and terrify in equal measure. The darker side has seen lawyers in the US fined for relying on fake, AI generated authorities. Closer to home a claimant's written submissions were found to contain a number of fake authorities leading to a wasted costs order[13]. The High Court has held a further hearing to investigate and it is not yet known if the cases were AI generated, but it does appear to be the most likely explanation. In defence of AI, it must be said that these examples reflect badly on the lawyers rather than the technology.

The Review does not shy away from the potential pitfalls of the use of AI in the disclosure process. Effective AI solutions are reliant on the quality and accuracy of initial input and there will always have to be someone accountable for the disclosure process, what the Review calls 'a rational human'[14]. The former can only be achieved through training and the use of specialist officers. This training must be properly funded, consistent throughout the criminal justice system and be reviewed and updated regularly. This all must form part of the recommended AI protocol.

The rational human with accountability is potentially more problematic. Of course, a disclosure officer and the OIC will remain accountable and available for explanations and cross-examination. But will such accountability bite if questions can be batted away with 'that's what the AI told us'? Could the use of AI allow the prosecution wriggle room or, worse still, could we end up with a Horizon situation where dogmatic belief in the infallibility of technology caused such widespread miscarriages of justice?

After all, the defence can't accuse AI it of misleading the jury in the witness box. Nor can AI be cross-examined about lost notebooks, overwritten CCTV or corrupted hard drives.

Clearly, as Jonathan Fisher KC writes, AI is capable of alleviating the burden of trawling through huge volumes of digital material. However, it is imperative that it's procurement, the human input and the real-life deployment is conducted properly at every stage.

Let us all hope that the Ministry of Justice adopts these technological recommendations in full and without delay. Being generous, the public sector's track record for rolling out technology is less than impressive. It would be a huge boost to the crumbling criminal justice system if it were to get this one right.

[*For the avoidance of doubt this article was not written by AI. However, in the interests of research ChatGPT was asked to comment and, inter alia, noted its balance: 'This balance makes the article credible and thoughtful, rather than tech-utopian or alarmist'. Rational humans can be the judge of that.]*

---

[12] https://www.gov.uk/government/news/initial-findings-of-our-e-discovery-review
[13] https://www.judiciary.uk/wp-content/uploads/2025/05/Ayinde-v-LB-Haringey-Judgment-Ritchie-J-03.04.25-HD-2.pdf at paragraphs 35-58
[14] The Review at paragraph 418 Page 130