The international journal of science / 25 January 2024

nature

Computers make mistakes — the law must recognize that

A tragic scandal at the UK Post Office highlights the need for legal change, especially as organizations embrace artificial intelligence to enhance decision-making.

More than 20 years ago, the Japanese technology conglomerate Fujitsu created an accounting software system for the UK Post Office. 'Horizon' was rolled out to branches across the country, often small, independently run shops that collect and deliver letters and parcels to tens of thousands of people. At the time, it was the largest civilian IT project roll-out in Europe. Horizon was beset by errors, a phase familiar to any user of a new IT system. Except, these were not irritatingly small bugs. In some cases, the Horizon IT system told members of staff that they were not depositing enough money at the end of a day's trading, leading to the 'loss' of thousands of pounds every night.

Many Post Office workers were accused of theft or false accounting. They were told to either pay the difference or face prosecution. More than 700 people were prosecuted, and an average of 30 were imprisoned each year between 2000 and 2014. Homes, livelihoods and relationships were wrecked. Some of those affected took their own lives.

Many details have yet to emerge. One of the most egregious is that Fujitsu said last week that it knew there were bugs in the system around the time it delivered Horizon to the Post Office in 1999.

However, one aspect of the scandal has attracted comparatively little attention: that the laws of England and Wales presume that computer systems do not make errors, which makes it difficult to challenge computer output. National and regional governments around the world where these laws exist need to review them, as there are implications for a new generation of IT systems — namely those using artificial intelligence (AI). Companies are augmenting IT systems with AI to enhance their decision-making. It is inconceivable to think that this is happening under legal systems that presume computer evidence is reliable. Until such laws are reviewed, more innocent people are at risk of being denied justice when AI-enhanced IT systems are found to be in error.

The core source of potential injustice with a law that presumes computer operations are fundamentally correct is that if someone wants to question or challenge computer evidence, the onus is on them to produce proof of improper use or operation. This could, for example, be through a record of the software's relevant code or keystroke logs. Yet, accessing this information is difficult. In most Horizon cases, defendants had no way of knowing which documents or records would show that a relevant error had occurred, and so could not request that these be disclosed by the Post Office when they were taken to court. This imbalance of knowledge meant that individuals had little hope of being able to defend themselves against the charges.

> "There are ways to establish transparency without revealing trade secrets."

Finding a way forward

Some lawyers and researchers involved in the defence of those prosecuted by the Post Office are advocating a different approach. Paul Marshall, a barrister at Cornerstone Barristers in London, and his colleagues argue in an article (P. Marshall *et al. Digit. Evid. Electron. Signat. Law Rev.* **18**, 18–26; 2021) that the presumption that computer evidence is reliable needs to be replaced with a requirement that relevant data and code will be disclosed in legal cases. When necessary, such disclosure should include information-security standards and protocols followed; reports of audits of systems; evidence showing that error reports and system changes were reliably managed; and records of steps taken to ensure evidence is not tampered with.

Relevant documents in the Horizon case were requested and produced when one group of claimants challenged the Post Office over being wrongfully accused. This group sought help from IT specialists and eventually won their case in 2019. By contrast, in individual cases in which defendants sought specialist help, the Post Office settled out of court, with defendants having to sign non-disclosure agreements — meaning that the computer evidence remained hidden.

The processes of IT systems can and must be explained in legal cases. There are ways to establish transparency without revealing trade secrets — a concern for some organizations and businesses. Sandra Wachter, a researcher in AI at the University of Oxford, UK, says that tools exist that can explain how automated systems make decisions, without revealing everything about how an algorithm works.

Back to the 1980s

During the 1980s — in the early days of personal computing — the law did not presume that a computer's operations were correct. Rather, proof to this effect was needed for computer-generated information to be allowed as evidence in courts. That law was changed in 1999 in recognition of the fact that the reliability of computers had improved — but the pendulum has swung too far in the other direction.

Complex IT systems using AI are increasingly making decisions that affect lives and livelihoods, from banking and finance to medical diagnoses, and from criminal justice to self-driving cars. As AI technologies become mainstream, so will legal cases involving these systems.

Computer evidence cannot be assumed to be reliable, and relevant laws that make such a presumption must be reviewed, so that such a similar miscarriage of justice is never allowed to happen again.