nagalro
children seen and heard
Article in *Seen and Heard*, Volume 35 | Issue 3 | 2025

EDITORIAL

Legal Aid Agency Data Breach

On 30 April 2025, the Legal Aid Agency sent an email to solicitors who have legal aid contracts to inform them of a 'security incident', in which it was 'possible' that financial information relating to legal aid providers 'may have been accessed'. The email continued:

> '*We are not able at this time to confirm what, if any, information was accessed, but it is possible that payment information may have been accessed.'*

By 13 May, the Legal Aid Agency was able to announce that it had successfully undertaken 'a number of additional actions to bolster the security of our systems'. The optimistic tone changed dramatically on 19 May, when the Agency announced that, on Friday, 16 May, it had discovered that 'the incident was far more extensive than originally understood, with the group behind it also having accessed a large amount of information relating to legal aid applicants'. The Agency urged all members of the public who had applied for legal aid since 2010 'to safeguard themselves'. A statement in similar terms was also published on the GOV.UK website. It was only through this statement that we learned that the Agency became aware of the security breach on 23 April 2025, a full week before any announcement took place. The statement goes on to say:

> *'We believe the group has accessed and downloaded a significant amount of personal data from those who applied for legal aid through our digital service since 2010.*
>
> *'The data may have included their dates of birth, national ID numbers, criminal histories, employment status and financial data such as contribution amounts, debts and payments.'*

This is the extent of the disclosure from the Agency and the Ministry of Justice. It is hardly surprising that Richard Atkinson, the President of the Law Society of England and Wales, has described it as 'scarce and inadequate given the scale of this security breach'. On 20 May, an update from the Agency confirmed that there was no responsibility for individual firms of solicitors to inform their clients of the breach, which, for most small firms, would have been a Herculean task. The letter says that the Ministry of Justice is the data controller for the purposes of the Data Protection Act 2018 and that the Ministry has notified the Information Commissioner's Office 'and has notified data subjects through the public announcement on GOV.UK on 19 May'. No other steps are being proposed to inform members of the public whose personal data has been stolen. A statement from the Law Society argues that it is

the Legal Aid Agency's responsibility 'to contact all the legal aid applicants whose data has been compromised'.

The paucity of the information made available by the Agency and the Ministry of Justice means that we must work out for ourselves the potential consequences of the breach. Unlike a stolen painting or sculpture, stolen data can never be recovered. Once it has been taken away, copies will be available on the dark web forever. Because of the restricted availability of legal aid, following the enactment of the Legal Aid, Sentencing and Punishment of Offenders Act 2012, many of those applying for legal aid will have been involved in family proceedings. More than that, many of the applicants will have been children involved in care proceedings, adoption cases, Deprivation of Liberty applications and private law matters. The loss of this data, which we must assume to be included, since we are not told otherwise, is very grave indeed. For a professional to lose the personal data of one child in care and adoption proceedings would likely be the end of their professional career, but to lose every child's data for the last 15 years?

Hacking is often motivated by the chance to acquire money. We do not know the identity or nature of the hackers to guess what they were trying to achieve, but it is likely that solicitors' bank accounts would have been a primary target. The risks, however, go much further than this. There will be mothers and children who believe that they have successfully concealed themselves from violent abusers, only to learn that their location is now in the hands of criminals. Details of children, vulnerable to sexual exploitation, are likely to now be in the hands of organised crime. Abused children, who have been adopted far from their parents' home, may find that their abusive birth parents can purchase details of their current location. The announcement, on 4 June 2025, that the government has obtained an injunction to prohibit any sharing of the information obtained will be of very little comfort to those whose data is in the hands of criminals, particularly criminals based far from the UK and the jurisdiction of its courts.

The government's reticence about the scale and potential impact of the breach smacks of reputational protection above the safety of individuals. Putting a notice on the GOV.UK website is simply nowhere near enough. The website is hardly a noted social venue, and many of the most vulnerable may not have much grasp of English anyway. Bland suggestions that individuals should 'protect themselves' may mean that individuals will have to change their name and move house. Will the Secretary of State pay for all this?

Rodney Noon
July 2025