Table A: Potential risks arising from the use of remote technology and mitigating measures taken to protect your data, privacy, and confidentiality

Potential risk	Mitigation measures
Breach of privacy and confidentiality	▪ I suggest you choose a quiet and private/ confidential environment for participating in an interview/ focus group. ▪ If you do not feel you can speak freely, or feel too distracted by your environment, we can reschedule.
Participants or research topic are of interest to 'motivated intruders' (i.e. persons seeking information for personal/political gain).	I anticipate for this to be no/ low risk, for the following reasons: ▪ You would be interviewed in your capacity as judicial office holders for your professional rather than private views. ▪ You would not be invited to comment on individual court cases, government policy or otherwise sensitive/ controversial topics.
Excessive accumulation of personal data that is not necessary for the aims of the research.	▪ You would be invited to choose between the following remote means of participation in place of/ in addition to face-to-face participation: > Interviews: 1) online, 2) via telephone, or 3) via e-mail. > Focus groups: 1) MS Teams, 2) MS Skype for Business, 3) Zoom. ▪ A choice of well-known and used online tools (MS Teams, MS Skype for Business, Zoom) would be offered. ▪ Video-calling would only be used if you agree to it. ▪ Recordings would be made only of audio, not video, and purpose-built encrypted voice recording devices not connected to the Internet would be used where possible/ appropriate. ▪ An interview guide focuses only those topics relevant to the research.
Interception and surveillance of communications that would not have been possible in a face-to-face setting.	▪ Only online tools managed by the University of Exeter (UoE) IT systems would be used. These offer a secure way of data gathering as data would be handled by the University IT systems. ▪ For interviews: To increase security in e-mail conversations, e-mail encryption would be considered and implemented where possible. I would use my UoE MS Outlook e-mail account, and suggest you use your e-judiciary e-mail account to make full use of our respective institutions' IT security systems. ▪ To increase security in telephone interviews, a dedicated SIM-card and phone would be used. A code word would be agreed for identity verification, where appropriate (esp. via telephone).
Breach of data protection policies, especially GDPR; loss of jurisdictional legal rights through transfer of personal data outside the EEA, EU and UK.	▪ The online tools used offer a GDPR- and UoE Information Governance policies-compliant way of data gathering. ▪ Data would be stored by MS Data Centres located in the UK and EEA/EU (https://docs.microsoft.com/en-us/office365/enterprise/o365-data-locations). The restriction of the Zoom server would be controlled by UoE IT. ▪ For telephone interviews, no messenger apps that could transfer data outside the EEA/ EU/ UK would be used.