Simon Dennis, Director, Future Government and Public Affairs, SAS UK&I — Written evidence (NTL0041)

1. SAS is the global leader in AI and Analytics and partner to governments and private enterprises who want to make better decisions faster. SAS uses artificial intelligence and analytical software to enable fully informed, consistent decisions to be taken throughout organisations based on the sum of institutional knowledge. This can take the form of crucial insights and predictions that can be distilled from the data to make evidence the basis for board level or policy decisions right down to automated split-second machine-decisions to perhaps honour a card-payment at point of sale, authorise a benefits claim or flag a vehicle for customs inspection. Both ends of the scale utilise the same data and each informs the other accordingly.

a. Our clients include over 90% of Fortune 500 companies and most major Government Departments globally. UK Key customers include HMRC's where our technology underpins risk and compliance management for the nation's finances, MoD as the data-analytics engine at the heart of efforts to save billions in asset and infrastructure costs and Ministry of Justice and Home Office whose custodial facilities benefit from "customer intelligence" to keep these facilities safe.

b. SAS submits this evidence in good faith based upon our experience of working with criminal justice agencies across the globe and our expertise in delivering innovation through our technology to both private and public institutions. As such we declare an interest as both an existing supplier and a potential future supplier.

SAS UK&I Response to Inquiry

Q1. Do you know of technologies being used in the application of the law? Where? By whom? For what purpose?

2. As the global leader in Artificial Intelligence and Analytics (as published by IDC), SAS supports hundreds of customers around the world ranging across the criminal justice sector.

3. Applications that we support include visual intelligence management which collates and organises all information relating to cases and identifies links and anomalies in support of investigations. AI is used to augment this data with open source intelligence and analytics are used to help focus investigators on material facts by removing distracting coincidental information. These applications are used by local and national police forces, financial crime and counter-fraud agencies, internal investigation functions, national criminal bureaux, the intelligence community, trading standards environmental enforcement and others. Crime reduction initiatives use AI to learn from historical records and so enable commanders to anticipate problems and ensure prevention initiatives are put in place.

4. In prisons and other supervised custodial environments, we ensure intelligence on the population is appropriately shared and AI is used to

identify patterns of behaviour that may indicate unsanctioned associations and hence identify potential risks of harm and illicit behaviour. In probation services AI is used to better target assistance to parolees and reduce recidivism.

5. Whilst the latest technologies may offer interesting possibilities, aside from the hyperbole emanating from tech start-up bubbles, the reality is that (outside China) the production-scale adoption of technologies such as Specialised Artificial Intelligence (SAI) or Machine Learning (ML) or Computer Vision (CV) in direct policing remains sparse. However, in the spirit of this inquiry, the committee may wish to broaden their scope to consider the legislative impact of innovative applications of existing technologies which present similar opportunities and associated risks and oversight challenges.

6. **The area of open systems and data fusion are key topics in this respect. Whilst data integration and exploitation are less glamourous than the aforementioned technologies, their application potential is vast and even now remains underexploited in conventional law enforcement**. Furthermore, the same data curation process is a necessary precursor to many of the AI-enabled capabilities under review and thus attention to getting these foundational aspects right in both execution and policy terms will create favourable conditions from which to build forward.

Q2. What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

7. Compliance with the law and acceptance of the authority exercised in its enforcement is ultimately based on the consent of the public. This consent relies on common societal values being the basis of imposed regulations coupled with the belief that powers conferred to enforce are proportionate to the risks to society posed by potential infractions.

8. **The aim of introducing new applications of technology will fall broadly into two overlapping categories:**

   a. Those that automate and reduce mistakes in existing complex, error-prone and time-consuming tasks and/or digitally facilitate collaboration and understanding.

   b. Those that use advanced computing methods to infer or estimate information or insight not already present in evidence or derive probabilistic intelligence used to inform an investigation or form elements of evidence used for prosecution.

9. New technologies in either category increase the power of the state apparatus and so diminish the freedoms of the wider population in a generalised sense, and this must be balanced against their value in preventing, detecting, investigating breaches and bringing offenders to justice.

10. **Category I** applications can be illustrated by Police Scotland's Digitally Enabled Police Programme which aims to improve the efficiency and effectiveness of its officers, by reducing the repetitive, time-consuming manual processes that ultimately delay situational understanding and reduce the accuracy and timeliness of operational decisions.

11. Typically, these processes seek to piece together fragments of information from a variety of data sources and types, both internal and external, and from either partner agencies or commercial data vendors. This mirrors existing manual processes to build up a view of the people, locations, vehicles, phone records, associations, statements and so forth.

12. As this programme progresses it will enable Police Scotland to move to a real-time data-ingestion and assimilation process and this will help keep people safe by addressing risks or solving cases earlier and with less false alarms.

13. **Category II** applications can be illustrated by an Offender Supervision Agency in North America that initially used data to better understand the agency's performance. Their staff data gave a good impression of the effectiveness of their supervision but when additional offender data were added it was identified that some staff would only target parolees with low perceived recidivism risk so providing a misleadingly rosy picture.

14. The agency subsequently developed this application to determine the risk of recidivism and how this was affected by environmental factors over time and so this became a tool for allocating parolees to staff more equitably. The application moved to Category II when the system went on to be used for targeting certain interventions such as work skills training or enhanced supervision activities at critical risk points in a parolee's journey. This was machine learning and was used with huge success.

15. The tool soon became invaluable in proving the success of their work and went on to support budget allocation and bidding for additional funding.

16. However, a nearby State heard about this application and asked for a demonstration on providing predictive information about parolees to their probation service. It quickly transpired that they had a different use in mind. They believed this would be a useful tool for probation boards in making their deliberations as whether to grant release.

17. The account team in the field withdrew from the engagement as it was inappropriate. Such a use would have been being ethically and morally wrong as well as being technically invalid but the well intentioned officials in this example did not have the relevant experience to make such a distinction.

Q3. Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers and members of the public) understand how they work and how they should be used?

18. The first aspect of this question depends heavily on the latter. Generally, technologies used in the application of the law should produce reliable and consistent outputs. However, this is based on an expectation that the quality of the input data is consistent with the requirement and then that the interpretation of the output is competent and appropriate.

19. The stereotypical misuse of statistics has largely been viewed as the shared domain of the media and politicians and it has never before been a requirement to have expertise in data science or statistics to be considered effective as a police officer, lawyer or judge.

20. Yet, it is the general population's poor grasp of the subject that makes this practice so effective and, because criminal justice professionals are typically also lacking an expert, or even good, understanding., It is a reasonable assumption that they may lack the necessary background for it to be certain that the technology is being used within safe/reliable operating parameters.

21. Given that information will often be synthesised as a machine estimate then procedures should be in place to ensure that the meaning of any such output is not only understood but that any limitations on its use or its quality as evidence are also clear, documented and that set procedures are followed to monitor compliance and identify misuse so that appropriate education and re-testing can be targeted.

Q4. How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated?

22. Misuse or abuse of technology will undoubtedly diminish trust in law enforcement, but technology also has the potential to increase trust in the law as it brings a scientific basis to its application. Modern alcohol detection technology paved the way for a fundamental reversal of public attitudes to driving under the influence of alcohol. Previously the level of intoxication had been subject to word-of-mouth self-assessment by the motorists or even their ability to perform certain acts of dexterity under the subjective view of the attending police officer.

23. A modern example of a positive application might be VIOGEN, a novel application at the Spanish Interior Ministry, that uses machine learning to help prevent the victims of gender-based violence from ongoing attacks from their aggressors.

24. This system has made a significant impact in ensuring that those at risk are given the appropriate protection. Police resources are scarce but after increasing the accuracy of prediction from 36% to 84% it has been possible to target these resources effectively.

25. The risk of miss-classifying a case where there is then an unexpected recurrence is perhaps the greater risk here, since no police protection would be offered to a victim who may be attacked again, these misfortunes currently run at 10% of cases but early results indicate that this can soon be reduced to 3%.

26. This system protects the victims and also ensures those who are not likely to be repeat offenders are spared from unwarranted police intrusion and thus increases acceptance and fosters increased faith in the police.

27. In both these cases the technology exhibited two key attributes:

a. The accuracy or quality of the results was sufficiently high to gain acceptance.

b. The system spared the rehabilitated offender as well as helping to identify those with a high potential to re-offend contributing to a sense of fairness in operation.

Q5. With regards to the use of the technologies, what costs could arise? Do the benefits outweigh these costs? Are safeguards needed to ensure that technologies cannot be used to serve purposes incompatible with a democratic society?

28. Whenever authorities sanction the use of technologies that encroach on individual freedoms, their potential impact on individual rights and more importantly their potential to override established democratic safeguards must be very carefully considered.

29. Omni-channel surveillance offers an enormous wealth of insight into an individual's beliefs, finances, sentiments, political views, vulnerabilities, movements etc. This is commercially very valuable and a powerful marketing tool but in the hands of the state apparatus it gathers a more sinister note given that regulations may have been employed to obtain key data or it had been provided for certain specific purposes only. Corrupt misuse of such systems offers organised criminals this same power and its use by hostile states or its agents is an equally unattractive prospect.

30. The range of opportunities for corrupt misuse of intelligent systems are extensive and whilst this general risk extends beyond the scope of this inquiry, the special case should be considered carefully due to the implications of the consequences of manipulating the criminal justice system.

31. Of course, the temptation to misuse such systems can also occur at the individual level and the opportunity to manipulate a system to create a derivative downstream effect should also be considered.

32. Indelible audit logging, pro-active oversight and proportionality are all critical to mitigating and diminishing, this risk.

Q6. What mechanisms should be introduced to monitor the deployment of new technologies? How can their performance be evaluated prior to deployment and while in use? Who should be accountable for the use of new technologies, and what accountability arrangements should be in place? What governance and oversight mechanisms should be in place?

33. The public, courts and politicians expect that law enforcement activities using new technologies will be legal, ethical and in line with human rights

legislation. They also expect that these systems will be managed with the highest levels of integrity.

34. Unfortunately, the threat of complacency, compromise and corruption is always high. In seeking to gain greater access and insight into criminal networks, there is potential for officers to be over-zealous or even manipulate others to commit crimes they wouldn't have otherwise committed. The temptation to act inappropriately based on probabilistic forecasts is sizeable and the insights these systems produce have high value to opposing criminal gangs. When things go wrong, the public's confidence in policing is eroded and the technology is withdrawn in an effort to stabilise confidence.

35. The risk of misuse is present across many information sources that are used in criminal justice and a particularly key example is human intelligence. HUMINT is a function that most policing and intelligence agencies operate– that is, people who form and use relationships with others to obtain or provide the agency with access to behind-the-scenes information. Agencies refer to these operations as covert human intelligence sources (CHIS). Operating practices, procedures and legislative requirements governing CHIS activities are different for every agency.

36. CHIS operations face the same challenges that new technologies face but to make matters worse, compromised sources are at substantial risk of violence. Every agency's goal must be to protect their sources, their handlers and their reputation.

37. In CHIS it is new technology itself that now provides part of the solution to ensuring compliance and this same model is a potential answer here as well.

38. Data and analytics technology enables tightly governed processes compliant with legislation, policies and national standards to be rigorously monitored and enforced while also providing intuitive dashboard views that can reveal insight into activities across the organizational ecosystem.

39. In the case of CHIS, technical challenges with gathering intelligence have intensified, making traditional informant handling increasingly necessary. But there are inherent risks in cultivating, recruiting, handling and managing human sources. Advanced proactive analytics technologies can quickly identify and alert on escalating risks or anomalies in handler or source behaviours.

40. Ideally, similar systems could be put in place for overseeing new technologies that cover operations, ranging from initial authorization to trial new technologies, ongoing conduct of investigations and the follow on use of derived information and eventual retirement from service use should that become appropriate.

41. These systems also oversee and evaluate performance of departments – and identify HR issues and training needs in the use of technology assets. This enables authorities to configure their risk assessment processes to match the specific capabilities individually and in ensemble.

Q7. How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks?

[no answer]

Q8. How far can transparency be ensured when it comes to the use of these technologies, including regarding how they are purchased, how their results are interpreted, and in what ways they are used?

42. Recently, COVID-19 technology procurements have allegedly involved multi-million pound contracts being awarded to inexperienced vendors, or those who should not have passed basic tests to weed out unfit businesses, posing a stark warning to our democracy.

43. The recent acceleration in the erosion in the public's faith in government following these highly publicised episodes needs urgent action to reverse it and so ensuring transparency across government is thus paramount.

44. It is a fundamental role of Parliament to protect our democracy whilst enabling technological innovation to be brought into service for the public. Where unconventional procurement routes are allowed to flourish this not only serves to undermine general public trust but also provides opportunities for unsavoury, unethical, illegal or hostile parties to deploy technologies with reduced scrutiny that can be misused or that harbour trojan-horse functionality or back-door routes to influence the outputs or decisions that such systems will increasingly perform.

45. Malign use of systems whose erstwhile purpose is benign requires that systems generate audit logs and that these logs are actively scrutinised by automated intelligent alerting systems that can flag suspicious activities to an appropriate oversight function and an independent body should receive

46. Appropriate safeguards or compensatory schemes for whistle blowers is an important factor in early corrective action and should be championed to avoid an ongoing series of crowd-funded and reputationally damaging court actions whenever transparency is threatened or breached.

Q9. Are there relevant examples of good practices and lessons learnt from other fields or jurisdictions which should be considered?

47. We would be happy to provide the committee with whatever additional advice or specific recommendations for criminal justice applications in which we have experience and will gladly broker direct contact with end users by mutual agreement in accordance with privacy regulations as appropriate.

Q10. This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend?

48. Key Themes to consider include:

   a. Overt

  b. Proportionate
  c. Technically Robust
  d. Independently Reviewed
  e. Monitored Actively
  f. Interpretable
  g. Secure
  h. Transparent

49. Thank you and SAS would be happy to provide additional evidence upon request.

10 September 2021