Insurance & Legal Report

2019

flourish

EMPOWERMENT THROUGH TRUSTED SECURE MOBILITY

M 4 (E)
London
Bristol (C)
(M32)
M 4 (W)
S. WALES
Chepstow
(M48)
The SOUTH WEST
Bristol (W) &
Filton (A38)
M 5
15

Contents

FLOURISH is a multi-sector collaboration, helping to advance the successful implementation of Connected and Autonomous Vehicles (CAVs) in the UK, by developing services and capabilities that link user needs and system requirements. The three year, £5.5 million project, seeks to develop products and services that maximise the benefits of CAVs for users and transport authorities. By adopting a user-centred approach, FLOURISH will achieve a better understanding of consumer demands and expectations, including the implications and challenges of an ageing society.

FLOURISH will address vulnerabilities in the technology powering CAVs, with a focus on the critical areas of cyber security and wireless communications. The project is trialled in the Bristol and South Gloucestershire region and is part funded from the government's £100 million Intelligent Mobility fund, which is administered by the Centre for Connected and Autonomous Vehicles (CCAV) and delivered by the UK's Innovation Agency, Innovate UK.

The FLOURISH consortium is made up of organisations from various sectors:

Joint Foreword

The three year FLOURISH project comes to an end this May. It has been three years of tremendous advancement for the CAV sector which has undoubtedly been contributed to by the work of FLOURISH partners both within their roles on this project, but also in their work outside of the project.

We have seen notable developments in cyber security and data protection, not least the introduction of the General Data Protection Regulation (GDPR) which has re-shaped the approach to the processing of personal data. The advancements over the past three years have contributed to the UK's position in the global CAV market and we have been pleased to see the Government's unwavering commitment to ensuring that the UK retains this position.

This report focuses on developments in the past year in cyber security and data protection. It examines some of the cyber security challenges of emerging technologies and explores some of the specific risks to the CAV sector. One of the key developments over the past year has been the publication by the British Standards Institution (BSI) of a new automotive cyber security specification, PAS 1885, for connected vehicles. This is an important development and one which demonstrates the UK's commitment to CAV technology.

In our Year 1 and Year 2 reports, we covered some key aspects of the GDPR and its application to the CAV sector. In this report, we highlight the principles of GDPR and set out our key principles for ensuring data protection compliance in the development of CAV products and services. We have designed these principles to work with the GDPR principles but with specific application to the work of stakeholders in the CAV ecosystem. It remains fundamentally important that we start to address the core questions around the availability of data and access rights to that data and we are encouraged by developments in this area, notably being led by the BSI and the CCAV.

It would be remiss of us to publish our third report without reiterating the role of law and insurance in the development of the CAV ecosystem. Law and insurance must be seen as an enabler; they should unlock opportunities whilst protecting people by balancing the collective good with individual requirements, providing clear accountabilities and risk allocation. As we note in our conclusions, both Burges Salmon and AXA remain committed to contributing to the development of legal and insurance frameworks which support the successful adoption of CAVs and ultimately, the UK's position as a world-leader in the CAV sector.

We would like to thank all of our FLOURISH partners for their work over the past year. We would also like to thank our colleagues for their work on FLOURISH over the past three years and, most recently, on this report. In particular, our thanks go to Lucy Pegler and Alicia Park at Burges Salmon and Sophie Bonnel and Jonathon Murphy at AXA.

May 2019

Chris Jackson
Head of Transport Sector
Burges Salmon LLP

David Williams,
Managing Director,
Underwriting
& Technical Services
AXA Insurance

CHAPTER 1:

Cyber Security

In our Year 1[1] and Year 2[2] reports, we considered the importance of cyber security for the development of CAVs. Throughout the running of the FLOURISH project we have seen a number of high-profile cyber security incidents highlighting the vital need for all parties involved in the CAV ecosystem to better understand how to improve and maintain vehicle cyber security. Safeguarding cyber security is crucial to ensure the UK can harness the benefits of the CAV market, which is estimated to be worth £52 billion to the UK economy by 2035.[3]

Security Challenges

Each year the European Union Agency for Network and Information Security (ENISA) identifies the key cyber security threats, which will be of relevance to developers and operators of autonomous systems. As highlighted in the ENISA 2018 report on emerging technologies,[4] the primary security challenges for autonomous systems emerge from resilience requirements, trust requirements and integrity requirements, with primary emphasis placed on trust, considering CAVs will *"probably be critically dependent on information exchanges with the outside world"*.

In the wider cyberthreat environment, ENISA identified a number of trends including:

- Mail and phishing messages have become the primary malware infection vector.
- Technical orientation of most cyberthreat intelligence produced is considered an obstacle towards awareness raising at the level of security and executive management.
- The emergence of Internet of Things (IoT) environments will remain a concern due to missing protection mechanisms in low-end IoT devices and services. The need for generic IoT protection architectures/good practices will remain pressing.
- The absence of cyberthreat intelligence solutions for low-capability organisations/end-users needs to be addressed by vendors and governments.[5]

Going beyond these main trends, we are acutely aware that CAVs sit within the IoT environment which is characterised by a complex interconnected ecosystem of devices and cloud-backed services likely to have a significant number of points of vulnerability. ENISA have identified a process gap in the security and privacy of an IoT product and service, even though there is no significant standards gap.[6] This gap is the result of standards not being treated holistically, meaning that whilst an IoT product or service can be deemed secure when tested against current standards, the product or service in the context of the entire system is still insecure. ENISA have found that the lack of cohesion on standards mean that interoperability is not a guaranteed outcome of IoT products and services even if security features are enabled. The security challenge for CAV developers and regulators is to analyse IoT devices in the context of a dynamic CAV ecosystem.

The House of Lords and House of Commons Joint Committee on National Security Strategy published their Third Report of the Parliamentary Session in November 2018; it focused heavily on the security challenges for the UK's critical national infrastructure (CNI). The CNI was stated to be a natural target for a major cyber attack due to its societal and economic importance; the threat was described as both growing and evolving. Critical cyber security threats cited by the Joint Committee included state-sponsored cyber espionage and theft of intellectual property from states and organised crime groups, with the challenge to fully secure CNI networks rendered impossible due to *"fast-changing threats and the rapid emergence of new vulnerabilities."*[7]

[1] FLOURISH, Insurance and Legal Report (2017) http://www.flourishmobility.com/storage/app/media/publication/J381379_Brochure_Flourish%20Report_V14_SPREADS.pdf
[2] FLOURISH, Insurance and Legal Report (2018) http://www.flourishmobility.com/storage/app/media/FLOURISH_Insurance_and_Legal_Report_2018.pdf
[3] HM Government Market Forecast: For connected and autonomous vehicles (2017)
[4] ENISA, Looking into the crystal ball: A report on emerging technologies and security challenges (2018) https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball
[5] ENISA, Threat Landscape Report 2018 (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[6] ENISA, IoT Security Standards Gap Analysis (2019) https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

According to ENISA, the top cyber security threats include:

Malware – malicious software that disrupts or damages IT systems such as banking Trojans and key-loggers. ENISA found that malware continues to be the most frequently encountered cyberthreat and involved in 30% of all data breach incidents and interestingly for the CAV ecosystem, ENISA also found that malware authors are increasingly targeting IoT devices and critical infrastructure.[8] The dependent nature of CAVs on software and external information exchanges means malware represents a significant threat to functionality and data-sharing.

Denial of service (DoS) – a DoS attack originates from a singular source, attackers aim to disrupt the availability of a service for legitimate users by flooding the IT systems with information.[9] CAVs are dependent on the connected services, the IoT and the sharing of data, therefore the increasing use of DoS attacks to disrupt services such as connected hospitals[10] is of importance for CAV stakeholders.

Data breaches – this term describes the result of a successful malicious cyberattack rather than a type of attack itself and often results in data being compromised or lost.[11] Experian in their 2019 forecast for data breaches illustrated that trends could include attackers exposing the vulnerabilities of biometric security systems and the security of wireless carriers.[12] As we have consistently highlighted in our Year 1 and Year 2 reports, the security of data is integral to the CAV ecosystem.

Information Leakage – the term covers both the accidental and unintentional distribution of sensitive and confidential data to an unauthorised entity resulting in the information becoming compromised.[13] The data can include both personal and commercial data. The most prevalent reason often stated for information leakage is unintended disclosure.[14]

Cryptojacking – the term refers to the unauthorised use of connected devices to mine for cryptocurrencies without the victim's consent.[15] ENISA highlight a clear shift from ransomware to cryptojacking due to its simplicity, lower risk and minimal law enforcement attention.[16]

The UK CAV landscape – the UK government has consistently announced that it wishes to see fully autonomous vehicles on UK roads by 2021.[17] In alignment with the investment of a £250 million programme of funding to support the development, demonstration and deployment activity through the CCAV[18], the UK government has placed an emphasis on the importance of cyber security especially in relation to autonomous vehicles and other IoT products and services.

[7] Joint Committee on the National Security Strategy, Cyber Security of the UK's Critical National Infrastructure: Government Response to the Committee's Third Report of Session 2017-2019 (2018) https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/2003/2003.pdf
[8] ENISA, Threat Landscape Report 2018 (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[9] Center for Internet Security, Technical White Paper – Guide to DDoS attacks (2017) https://www.cisecurity.org/white-papers/technical-white-paper-guide-to-ddos-attacks/
[10] ENISA, Threat Landscape Report 2018 (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[11] ENISA, Threat Landscape Report 2018 (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[12] Experian, Data Breach Industry Forecast 2019 (2019) https://www.experian.com/assets/data-breach/white-papers/2019-experian-data-breach-industry-forecast.pdf
[13] A. Shabtai et al., "A Survey of Data Leakage Detection and Prevention Solutions" Springer Briefs in Computer Science, 2012
[14] Privacy Rights Clearinghouse, Data Breaches (2018) https://www.privacyrights.org/data-breaches/breach-type?taxonomy_vocabulary_11_tid=2436
[15] Norton, What is cryptojacking? How it works and how to help prevent it (2019) https://us.norton.com/internetsecurity-malware-what-is-cryptojacking.html
[16] ENISA, Threat Landscape Report 2018 (2019) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018
[17] HM Government, Industrial Strategy – Building a Britain fit for the future (2017) https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future
[18] Centre for Connected and Autonomous Vehicles, About us (2019) https://www.gov.uk/government/organisations/centre-for-connected-and-autonomous-vehicles/about

The UK's Industrial Strategy[19]

The Industrial Strategy was published in November 2017 and is the UK Government's long-term plan to create an economy that boosts productivity and earning power throughout the UK. In its strategy the UK Government identifies **five "foundations of productivity"** i.e. those attributes essential for a successful economy:

1. **Ideas** – the world's most innovative economy.
2. **People** – good jobs and greater earning power for all.
3. **Infrastructure** - a major upgrade to the UK's infrastructure.
4. **Business Environment** – the best place to start and grow a business.
5. **Places** – prosperous communities across the UK.

The Government aims to put the UK at the forefront of technologies of the future by setting 'Grand Challenges' for UK government and the wider economy. The **four Grand Challenges** as set out in the UK's Industrial Strategy are:

1. Putting the UK at the forefront of the artificial intelligence and data revolution;
2. Maximising the advantages for UK industry from the global shift to clean growth;
3. Being a world leader in shaping the future of mobility; and
4. Harnessing the power of innovation to help meet the needs of an ageing society.

The UK

On the wider issue of IoT cyber security the Department for Culture, Media & Sport and the National Cyber Security Centre in October 2018 released a Code of Practice for Consumer IoT Security (the **Code of Practice**) [20] for parties involved in the development, manufacturing and retail of consumer IoT, with guidance for consumers on smart devices at home.
The scope of the Code of Practice applies to home and personal devices such as health trackers, smart TVs and safety-relevant home products. The Code of Practice includes guidelines recommending companies implement a vulnerability disclosure policy, ensure software is securely updated and ensure systems are resilient to outages of data networks and power.

More specifically focused on the CAV sector and cyber security risks, in the recent report released by the Department for Transport (DfT) entitled 'Future of mobility: urban strategy' the Government clearly recognised the risk of cyber threats to CAVs in their description of how the UK can shape the future of mobility as part of the wider industrial strategy:

"Closer integration of our infrastructure and vehicles with communication networks could lead to increased vulnerability to cyber-attacks. As new transport modes and services are introduced, it will be important to consider how they can be safely integrated into the transport system, and vulnerable users can be protected." [21]

This point was also a clear feature of the Government's new Code of Practice [22] released by CCAV for automated vehicle trialling. The Code included two key cyber security guidelines for manufacturers and trialling organisations:

- Manufacturers providing vehicles, and other organisations supplying parts for trials will need to ensure that all vehicle systems have appropriate security measures to manage data security and the risk of unauthorised data access. Trialling organisations are recommended to follow the UK government's Key Principles of Cyber Security for Connected and Automated Vehicles and should also consider adopting BSI PAS 1885:2018. The fundamental principles of automotive cyber security specification in addition to the other relevant standards and guidance that are referenced in each of these documents. These consider the development and production of trial vehicles, in addition to organisational factors that would contribute to the overall security of the operation. [23]

- Trialling organisations should consider adopting the security principles set out in BS 10754-1:2018 (Information technology – Systems trustworthiness. Governance and management specification). [24]

[19] HM Government, Industrial Strategy – Building a Britain fit for the future (2017) https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future
[20] Department for Digital, Culture, Media and Support, Code of Practice for Consumer IoT Security (2018) https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
[21] Department for Transport, Future of mobility: urban strategy (2019) https://www.gov.uk/government/publications/future-of-mobility-urban-strategy
[22] Department for Transport, Department for Business, Energy & Industrial Strategy and Centre for Connected and Autonomous Vehicles, Trialling automated vehicle technologies in public (2019) https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public
[23] British Standards Institution, PAS 1885: The fundamental principles of automotive cyber security (2018) https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114
[24] British Standards Institution, BS 10754-1: 2018 Information technology. Systems trustworthiness. Governance and management specification https://shop.bsigroup.com/ProductDetail?pid=000000000030351844

Key Principles

In our Year 2 report we discussed in detail the *Key principles of Cyber Security for Connected and Automated Vehicles* that were announced by the Government in August 2017. [25]

The eight principles remain:

1. Organisational security is owned, governed and promoted at board level.
2. Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.
3. Organisations need product aftercare and incident response to ensure systems are secure over their lifetime.
4. All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.
5. Systems are designed using a defence-in-depth approach.
6. The security of all software is managed throughout its lifetime.
7. The storage and transmission of data is secured and can be controlled.
8. The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

It is evident from the eight principles that the focus is placed on board-level management, accountability and transparency throughout the life-cycle of the CAV ecosystem including their extended supply chains. Subsequent to the key principles, the BSI, in December 2018, released a new automotive cyber security specification, PAS 1885, for connected vehicles, funded by the DfT and in collaboration with academics and experts from car manufacturers and the National Cyber Security Centre. [26] The standard has been developed primarily to provide guidance to the stakeholders in the industry in order for them to be able to coherently demonstrate, throughout the life cycle of the automotive development, compliance with the DfT's key principles. In announcing the standard, the Future of Mobility Minister, Jesse Norman MP, stated that the *"cyber security standard should help to improve the resilience and readiness of the industry, and help keep the UK at the forefront of advancing transport technology."* [27]

BSI states that the concept of an automotive ecosystem encompasses:

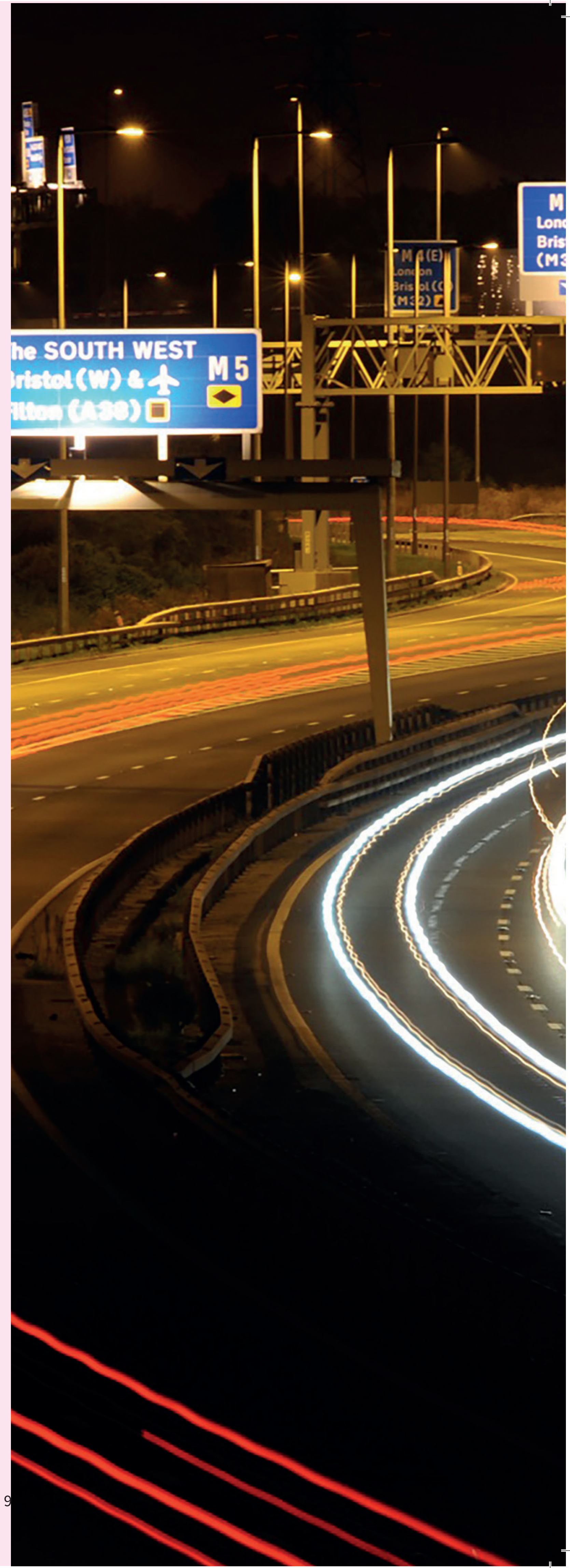
- Vehicles;
- Related infrastructure, including road-side and remote systems that provide services to the vehicles, their operators, occupants and cargo; and
- The human elements, including vehicle owners and/or operators, designers, manufacturers and service providers. [28]

Importantly, BSI PAS 1885 highlights the need for organisations to have a holistic approach to security which addresses five crucial domains of people, the physical environment, business processes, technology, data and information security issues and governance; and covers the eight security goals of confidentiality, availability, safety, resilience, possession, authenticity, utility and integrity. The need for a holistic approach is for organisations to understand both the security context and the inextricable links between cyber-security risks.

The standard goes through each of the eight principles to provide guidance for how best for an organisation's board-level management to ensure they are able to demonstrate they are following them. Although the standard is not mandatory, it does provide a marker for stakeholders developing self-driving car technology. A non-exhaustive list of **key guidance items** in the standard includes:

- The board-level management should establish a governance approach, governance structure and an organisation Security Strategy to manage security-related requirements and set out personal accountability for the ownership and management of security risks.
- The board-level management should establish, document and maintain a record of the organisation's risk appetite.
- The board-level management should develop, document and maintain an Asset-based Risk Register.
- The board-level management should develop, document, implement and maintain a Security Management Plan that addresses specific security objectives in the organisation's Security Strategy and the security risks identified in the Asset-based Risk Register.
- The board-level management should develop, document, implement and maintain a Security Incident Management Plan tailored to the organisation.
- The board-level management should develop, document, implement and maintain a Supply Chain Security Management Plan that defines the contractual and operational measures required for the adoption of an appropriate and proportionate security-minded approach throughout the organisation's supply chain.
- The board level management should develop, implement and periodically review an overarching policy regarding the sharing of data and/or information.
- The board-level management should establish and maintain a security program aligned to the organisation's Security Strategy to ensure a consistent approach.
- The board-level management should embed a security culture within its personnel and suppliers.
- The organisation's board-level management should establish, document and operate policies, processes and procedures such that all new designs are conceived and implemented using a product and/or service lifecycle that embraces Secure-by-Design. [29]

Throughout the FLOURISH project we have made a number of recommendations in terms of cyber security that we felt would be key to unlocking the societal benefits of CAV technology. [30] It is pleasing to see not only the Government incorporate many of these issues into their key principles but to also see the BSI collaborate with expertise in the sector to provide guidance on how these key principles can be followed. There are a range of cyber security risks and threats that must be prepared for as this technology develops, we recommend that stakeholders in the sector use the guidance incorporated in the PAS 1885 to develop a holistic and consistent approach and further welcome the work being done by the FLOURISH project to achieve the embedding of security into the entire lifecycle of CAV technology.



[19] HM Government, Industrial Strategy – Building a Britain fit for the future (2017) https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future

[20] Department for Digital, Culture, Media and Support, Code of Practice for Consumer IoT Security (2018) https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

[21] Department for Transport, Future of mobility: urban strategy (2019) https://www.gov.uk/government/publications/future-of-mobility-urban-strategy

[22] Department for Transport, Department for Business, Energy & Industrial Strategy and Centre for Connected and Autonomous Vehicles, Trialling automated vehicle technologies in public (2019) https://www.gov.uk/government/publications/trialling-automated-vehicle-technologies-in-public

[23] British Standards Institution, PAS 1885: The fundamental principles of automotive cyber security (2018) https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

[24] British Standards Institution, BS 10754-1: 2018 Information technology. Systems trustworthiness. Governance and management specification https://shop.bsigroup.com/ProductDetail?pid=000000000030351844

The Developing Legal Landscape

The second FLOURISH report highlighted a fast-developing legal landscape with the implementation of the General Data Protection Regulation (**GDPR**), [31] the Royal Assent of the Data Protection Act 2018 [32] and the implemented of the Network and Information Systems Directive into UK law as the Network and Information Systems Regulations (**NIS Regulations**).

Introduced in 2016 by the EU and implemented in the UK in May 2018, the NIS Directive aims to improve cyber security capabilities across the EU as a way of improving the overall resilience of network and information systems. [33] The regulation applies to operators of essential services (OES) and digital service providers (DSPs), with particularly strict compliance obligations set out for OES to ensure they "take appropriate and proportionate security measures to manage risks to their network and information systems". [34]

In March 2018, the National Cyber Security Centre issued guidance on implementing the NIS Directive which included four objectives and 14 principles: [35]

The four Network and Information Systems Regulations objectives:

- **A** Managing security risk
- **B** Protecting against cyber-attack
- **C** Minimising the impact of cyber security events
- **D** Minimising the impact of cyber security incidents

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[32] FLOURISH, Insurance and Legal Report (2018) http://www.flourishmobility.com/storage/app/media/FLOURISH_Insurance_and_Legal_Report_2018.pdf
[33] Department for Digital, Culture, Media & Sport, The NIS Regulations 2018 (2018) https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018
[34] Department for Digital, Culture, Media & Sport, Security of Network and Information Systems: Government response to public consultation (2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf
[35] National Cyber Security Centre, NIS guidance (2019) https://www.ncsc.gov.uk/collection/nis-directive

The fourteen Network and Information Systems Regulations principles

A1. Governance
The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.

A2. Risk management
The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services. This includes an overall organisational approach to risk management.

A3. Asset management
Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood. This includes data, people and systems, as well as any supporting infrastructure (such as power or cooling).

A4. Supply chain
The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers. This includes ensuring that appropriate measures are employed where third party services are used.

B1. Service protection policies and processes
The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.

B2. Identity and access control
The organisation understands, documents and manages access to systems and functions supporting the delivery of essential services. Users (or automated functions) that can access data or services are appropriately verified, authenticated and authorised.

B3. Data security
Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services. Such protection extends to the means by which authorised users, devices and systems access critical data necessary for the delivery of essential services. It also covers information that would assist an attacker, such as design details of networks and information systems.

B4. System security
Network and information systems and technology critical for the delivery of essential services are protected from cyber-attack. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures to effectively limit opportunities for attackers to compromise networks and systems.

B5. Resilient networks and systems
The organisation builds resilience against cyber-attack into the design, implementation, operation and management of systems that support the delivery of essential services.

B6. Staff awareness and training
Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.

C1. Security monitoring
The organisation monitors the security status of the networks and systems supporting the delivery of essential services in order to detect potential security problems and to track the ongoing effectiveness of protective security measures.

C2. Proactive security event discovery
Detecting anomalous events in relevant network and information systems.

D1. Response and recovery planning
There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.

D2. Lessons learned
When an incident occurs, steps must be taken to understand its root causes and ensure appropriate remediating action is taken.

The importance of the legal landscape and specifically the implementation of the NIS Regulations is that it is likely that in order for CAV operators to access roadways they will have to comply. Therefore, the guidance laid out above and subsequent guidance provided by relevant authorities will be of significance as CAV technology develops.

It should however be noted that the Joint Committee on National Cyber Security Strategy stated that although NIS Regulations offer a robust regulatory framework for CNI sectors, they are limited in scope, result in fragmented responsibility for Government implementation and some designated 'Competent Authorities' lack the expertise to provide credible assurance of operators' efforts. [36]

[36] Joint Committee on the National Security Strategy, Cyber Security of the UK's Critical National Infrastructure: Government Response to the Committee's Third Report of Session 2017-2019 (2018) https://publications.parliament.uk/pa/jt201719/jtselect/jtnatsec/2003/2003.pdf

Brexit

The UK Government confirmed in December 2018 that the NIS Directive will continue to apply in the UK after the UK completes its exit from the European Union. However, if the UK leaves the EU in a ‘no deal scenario’, relevant digital service providers in the UK that offer services in an EU Member State will be required to designate a representative in an EU Member State. [37]

The EU (Withdrawal) Act 2018 retains GDPR in UK law. The UK Government further confirmed in February 2019 that they will make appropriate changes to both GDPR and the Data Protection Act 2018 ensure the data protection framework operates effectively following the UK’s exit from the European Union. The amended regulation would:

- Transitionally recognise all EEA countries (including EU Member States) and Gibraltar as ‘adequate’ to allow data flows from the UK to Europe to continue.
- Preserve the effect of existing EU adequacy decisions on a transitional basis.
- Recognise EU Standard Contractual Clauses (SCCs) in UK law and give the ICO the power to issue new clauses.
- Recognise Binding Corporate Rules (BCRs) authorised before exit day.
- Maintain the extraterritorial scope of the UK data protection framework.
- Oblige non-UK controllers who are subject to the UK data protection framework to appoint representatives in the UK if they are processing UK data on a large scale. [38]

The Cyber Breaches Survey 2019 [39]

The Cyber Breaches Survey is conducted every year by the Department for Culture, Media and Sport as part of the Government’s National Cyber Security Programme. The **2019** report has findings that are revealing for understanding the significant threat of cyber attacks and business attitudes towards cyber security.

32% of businesses report having cyber security breaches or attacks in the last 12 months, this figure increases to **60%** and **61%** for medium and large businesses respectively.

The number of businesses updating their senior management on actions taken around cyber security at least once a quarter has increased by **6%** from **51%** to **57%**.

Written cyber security policies are more common among businesses, **33%** of respondents reported having a written policy up **6%** from 2018.

Only **35%** of businesses have a board member with specific responsibility for cyber security, **18%** require their suppliers to adhere to any cyber security standards and **16%** of businesses have formal cyber security incident management processes in place.

The average investment in cyber security in the last financial year for a business operating in the transport sector was **£7,730**, up from **£6,570** last year. However, this is still significantly less than the average spend of **£22,050** in the finance and insurance sector.

54% of businesses invest in cyber security to protect customer data, an increase of **7%** from last year.

[25] Department for Transport, Centre for the Protection of National Infrastructure and Centre for Connected and Autonomous Vehicles, Principles of cyber security for connected and autonomous vehicles (2017) https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles

[26] British Standards Institute, PAS 1885: The fundamental principles of automotive cyber security (2018) https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

[27] Department for Transport, Centre for Connected and Autonomous Vehicles and Jesse Norman MP, New cyber security standard for self-driving vehicles (2018) https://www.gov.uk/government/news/new-cyber-security-standard-for-self-driving-vehicles

CHAPTER 2:

Data and the Key Principles

In our Year 1 [40] and Year 2 [41] reports, we considered the importance of data in the functioning of the CAV ecosystem.

A recent report by the Society of Motor Manufacturers and Traders (SMMT) and Frost & Sullivan examined the benefits that may be realised through the deployment of CAVs on UK roads. [42] The report identified an annual economic opportunity for the UK of £62 billion by 2030 and identified three key areas of development which, the report suggests, will be instrumental to enabling the UK to realise the potential of CAVs.

Three key areas of development:

1. **Enabling Infrastructure:** deployment of communications infrastructure will be key to the success of CAVs and the report notes that whilst the UK has good coverage across its motorway network, it currently only has a 58% coverage range for A and B roads.
2. **Enabling Regulations:** the report [43] highlights the UK's progress in developing regulation fit for CAV deployment and in particular, the Automated and Electric Vehicles Act 2018. It goes on to note that the UK has a "strong policy intent on transport-related data aggregation and sharing, gathered by operators at a national level, authorised by the government".
3. **Market Attractiveness:** the UK scored well in the analysis of market attractiveness which looked at indicators for CAV adoption, in this case, Advanced Driver Assistance Systems (ADAS), connected cars, Mobility as a Services (MaaS) and Demand Responsive Transport (DRT).

In recognition of the value and importance of data, KPMG's 2019 Autonomous Vehicles Readiness Index [44] (the **AVRI**) this year added a new measure assessing the data-sharing environment. The AVRI praised the UK government's "forward-thinking approach" which has contributed to the UK being ranked second for policy and legislation and first for data-sharing.

The value of the CAV market to the UK is one of the many drivers for ensuring that an enabling regulatory framework is in place to support the deployment of CAVs on UK roads.

A core part of that enabling framework will be focused on the use of data; how will data of all types be collected, processed, shared and protected.

In our Year 2 report, we highlighted that the successful functioning of the CAV ecosystem will rely upon data sharing between stakeholders. We stressed that developing a robust framework for the sharing of data that achieves regulatory compliance in a manner that enables the ecosystem to function is highly important to this, but developing a framework which is understood and trusted by users is paramount.

The focus of our Year 2 report was data and the user and, in particular, we looked at how the CAV ecosystem will secure the trust of users. We also recommended that government and industry stakeholders collaborate to begin the exercise of structuring a 'data map' for the CAV ecosystem with the principle aim of exploring what data sharing may be required.

Having examined some of the challenges faced by users in sharing their data, it is necessary to consider some of the challenges faced by organisations in sharing data. For many organisations, increasing access to data will require a cultural shift – sharing data on the scale demanded for the effective functioning of the CAV ecosystem has for many years been resisted and although there are signs that this is changing, increasing access to data to enable optimisation of CAVs will require significant time and cost investment.

[28] British Standards Institution, PAS 1885: The fundamental principles of automotive cyber security (2018) https://shop.bsigroup.com ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

[29] British Standards Institution, PAS 1885: The fundamental principles of automotive cyber security (2018) https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

[30] FLOURISH, Insurance and Legal Report (2017) http://flourishmobility.com/storage/app/media/publication/J381379_Brochure_Flourish%20Report_V14_SPREADS.pdf

[37] Department for Digital, Culture, Media & Sport, NIS Regulation: EU Exit Guidance for digital service providers established in the UK (2018) https://www.gov.uk/government/publications/nis-regulation-eu-exit-guidance

[38] Department for Digital, Culture, Media & Sport, Amendments to UK data protection law in the event the UK leaves the EU without a deal on 29 March 2019, (2019) https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019

[39] Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2019: Main report (2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791940/Cyber_Security_Breaches_Survey_2019_-_Main_Report.PDF

[40] FLOURISH, Insurance and Legal Report (2017) http://flourishmobility.com/storage/app/media/publication/J381379_Brochure_Flourish%20Report_V14_SPREADS.pdf

[41] FLOURISH, Insurance and Legal Report (2018) http://www.flourishmobility.com/storage/app/media/FLOURISH_Insurance_and_Legal_Report_2018.pdf.

[42] SMMT and Frost & Sullivan 'Connected and Autonomous Vehicles – 2019 Report' (https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CONNECTED-REPORT-2019.pdf)

[43] Ibid

[44] KPMG '2019 Autonomous Vehicles Readiness Index – Assessing countries' preparedness for autonomous vehicles' (https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf)

The Open Data Institute (ODI):
As part of an ongoing project into how access to data can be increased while retaining trust, the Open Data Institute (ODI) last year interviewed organisations to understand the challenges organisations face when sharing data. [45] The ODI broadly categorises the challenges as:

- **Data discovery** – being able to identify relevant data and issues encountered where that data is in an unstructured and inconsistent format;
- **Data control and access** – who controls data and who has access to it;
- **Trust** – in particular, trust in data quality;
- **Transparency** – evidence of the benefits of sharing data; and
- **Business case** – identifying and understanding business models which support data sharing.

The ODI's observations on the data challenges in the transport sector are particularly relevant in the context of CAVs.

The ODI highlighted that ***"In the automotive industry, it's not clear who should control data generated by modern auto-mobiles. Access to the data could be claimed by drivers, passengers, car owners, car manufacturers, software or hardware providers, or the wider transport network". The report goes on to note that "In the Autonomous Vehicles sector, data from local authorities may be seen as more trustworthy than data from a private company"***.

Resolving some of these perceived challenges will be key to ensuring the effective sharing of data in the CAV ecosystem.

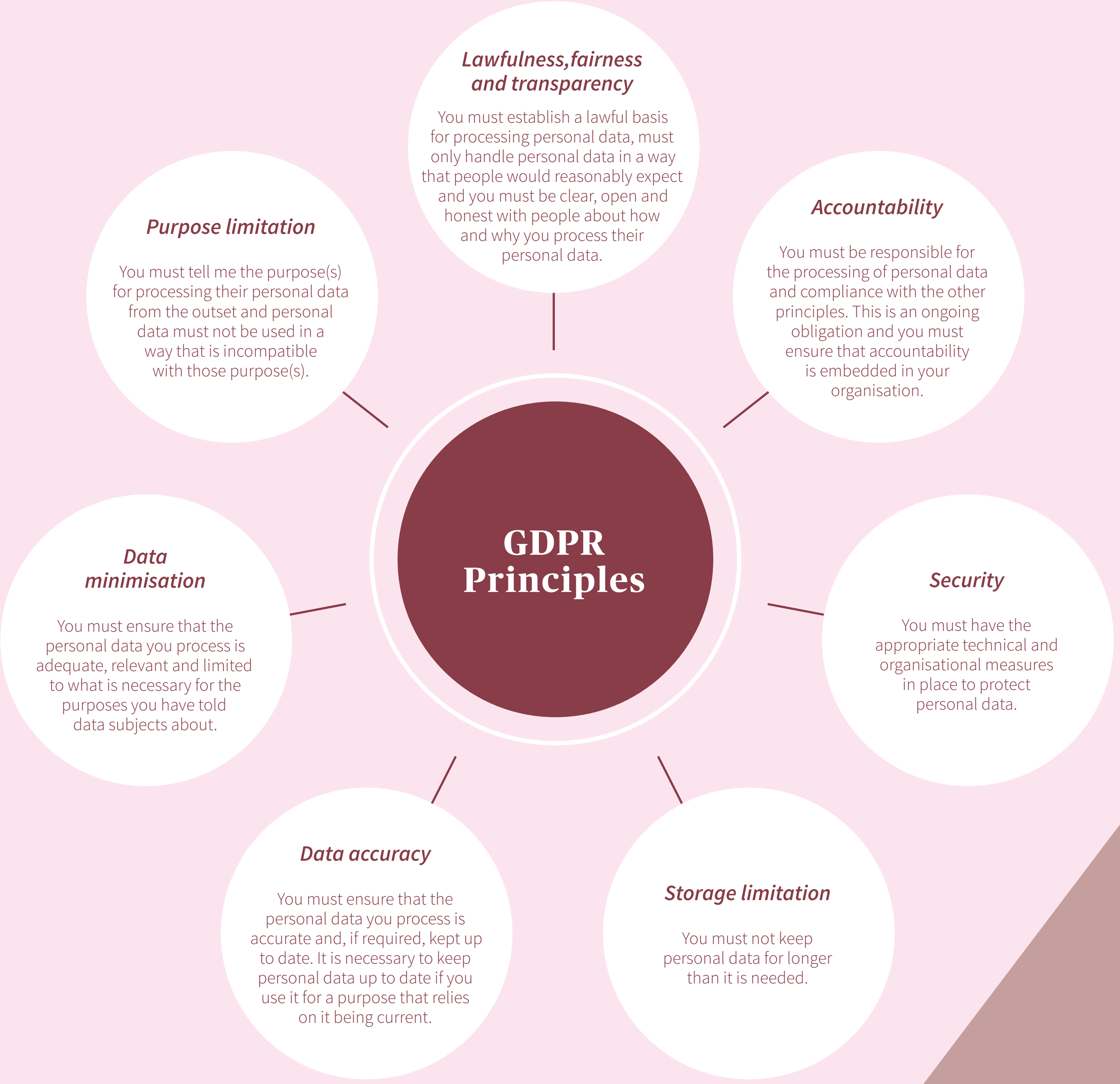
[45] Open Data Institute 'What organisations need in order to share more data: our research' (https://theodi.org/article/what-organisations-need-in-order-to-share-more-data-our-research/) accessed 11 April 2019

Building in good data protection practices: the GDPR principles

The CAV market is some way off having a developed framework to support the sharing of data but it is an area which has an ever increasing influx of support from key bodies such as the BSI and the CCAV.

However, in a period of rapid technological development, it is vital that there is a clear pathway for the development of technology which at its core respects and adheres to the principles that apply to the protection of personal data.

The GDPR sets out seven key principles which are fundamental to the processing of personal data. Any organisation processing personal data should be familiar with these principles and they will apply equally to the processing of personal data in the CAV ecosystem.



GDPR Principles

Lawfulness,fairness and transparency

You must establish a lawful basis for processing personal data, must only handle personal data in a way that people would reasonably expect and you must be clear, open and honest with people about how and why you process their personal data.

Accountability

You must be responsible for the processing of personal data and compliance with the other principles. This is an ongoing obligation and you must ensure that accountability is embedded in your organisation.

Security

You must have the appropriate technical and organisational measures in place to protect personal data.

Storage limitation

You must not keep personal data for longer than it is needed.

Data accuracy

You must ensure that the personal data you process is accurate and, if required, kept up to date. It is necessary to keep personal data up to date if you use it for a purpose that relies on it being current.

Data minimisation

You must ensure that the personal data you process is adequate, relevant and limited to what is necessary for the purposes you have told data subjects about.

Purpose limitation

You must tell me the purpose(s) for processing their personal data from the outset and personal data must not be used in a way that is incompatible with those purpose(s).

The principles set out in GDPR should be central to any processing of personal data. As we have explored in our Year 1 and Year 2 reports, whilst CAVs will generate an unprecedented volume of data, not all data will be personal data.

In its AVRI, KPMG highlighted the role of the *Key Principles of Vehicle and Cyber Security for Connected and Autonomous Vehicles* (as further discussed in Chapter 1 of this Report) in contributing to the efforts to ensure the safety of CAVs. [46] As we highlighted in our Year 2 report, if data is the new fuel then it follows that the success of the CAV ecosystem is, in part, dependent on securing the trust of users in particular in relation to the use of their data.

Ten principles for protection of data in the CAV sphere

We set out below a list of **ten key principles** for protection of data in the CAV ecosystem. These principles build in and elaborate on the GDPR principles. They are not exhaustive but are designed to support and guide stakeholders as they develop CAV products and services.

1 Take it to the top and ensure accountability

Accountability is a fundamental tenant of data protection legislation but it will be important to the sharing of all data (not just personal) in the CAV ecosystem.

Engage with your board and senior management. Organisations must not only take responsibility for compliance with the obligations under GDPR but they must also be able to prove their compliance.

What can you do in practice?
Keep accurate records and documentation. Document decisions, put written agreements in place with developers, manufacturers and other third parties that you work with. This is not exhaustive but the key is to start the process of documentation early on in the development stages and to continue it throughout the lifecycle of the development of products and services.

2 Recognise that one size does not fit all

In the development of CAV technology, understanding the potential for personal data to be collected and processed is crucial. In the early stages of research and development, clearly defined data sets will be unlikely and so developing technologies which permit a degree of flexibility will be key.

Any one system may be processing multiple categories of data. Applying the same level of security to all data may be unduly restrictive or unnecessarily risky.

3 Identify your lawful basis of processing

In order to process personal data, in other words, in order to do anything with data from which an individual can be identified, a data controller must be able to demonstrate a valid lawful basis. Our Year 2 report took a more detailed dive into this topic but, simply put, consent is unlikely to be a sufficient basis for processing in the CAV ecosystem because it must be capable of being withdrawn as easily as it is given. Therefore, the CAV ecosystem is likely to rely on a number of lawful bases, for example, fulfilling a contractual obligation with the individual or legitimate interests.

4 Build privacy by design

CAV technology should be developed to only collect data that is needed and is proportionate to requirements. Challenge your organisation and your partners: are you asking for too much data and does it all need to be identifiable? As far as possible data should be anonymised or pseudonymised to protect individual's rights.

[46] KPMG '2019 Autonomous Vehicles Readiness Index – Assessing countries' preparedness for autonomous vehicles' (https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf)

5 Data Mapping and DPIA (Data Protection Impact Assessment)

Organisations will need to carry out a full data mapping exercise to identify any data that will be processed during the lifecycle of the CAV. This may be a complex and involved process but it is essential in order to be transparent with customers and gain user trust in the CAV ecosystem.

In advance of carrying out any data analytics a data protection impact assessment should be carried out. This should consider the details of the processing that will be carried out, assess the proportionality of the processing and the measures that will be taken to ensure compliance, then identify the risks of that processing and how to mitigate those risks.

6 Follow cyber security best practice

All systems and services in the CAV ecosystem should have appropriate technical and organisational measures in place to protect personal data. Our second report [47] summarised the government's eight principles for cyber-security which include: promoting security at board level; ensuring risks are assessed and managed properly; having appropriate aftercare and incident response; working with relevant third parties to develop the safety of the system; ensuring the system is resilient to attacks, and so on.

Companies should also follow the UK Government's guidance (the *Key Principles of Cyber Security for Connected and Automated Vehicles*) and the BSI PAS 1885 (*The fundamental principles of automotive cyber security - specification*). [48]

7 Ensure integrity of data and access

It is important to remember that where you are processing personal data, end-users (i.e. data subjects) must be able to access their personal data in line with their rights under the GDPR. You should ensure that personal data is kept up to date and accurate; build in reminders for verifying the data you are holding.

Data integrity goes beyond personal data; the reliability of data is absolutely critical in the CAV ecosystem.

8 Customers must be informed

As customer trust is such an important issue and could be the "making or breaking" of the CAV industry, communicating how you intend to use customer data and the bases for doing so, is essential. How this is done will depend on how the customer interacts with you; it may be via registration on the internet or it could be via a user manual. In any case, customers should be informed of the processing that will take place and the bases for doing so, clearly and transparently. Organisations will be obliged to carry out a full data mapping exercise (see principle 9) so they can appropriately communicate with customers.

[47] FLOURISH, Insurance and Legal Report (2018) http://www.flourishmobility.com/storage/app/media/FLOURISH_Insurance_and_Legal_Report_2018.pdf

[48] British Standards Institute, PAS 1885: The fundamental principles of automotive cyber security (2018) https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114

[49] https://www.unece.org/info/media/presscurrent-press-h/transport/2019/autonomous-transport-must-be-developed-with-a-global-eye/doc.html and https://www.unece.org/info/media/presscurrent-press-h/transport/2019/countries-adopt-2030-strategy-for-sustainable-inland-transport/doc.html

9 Collaboration

Collaboration is critical. Ensuring that stakeholders are communicating, particularly when it comes to the use of data, is key. There will need to be ongoing conversations between CAV stakeholders regarding what data should be collected and what should be shared; channels of communication (between governments, OEMs, communication network providers and all other stakeholders in the CAV sphere) will be needed to ensure that communication is kept open and ongoing. This builds on the idea that data sharing will be key to the development of the industry and its efficiencies; Discussions around safely sharing appropriate levels of data will need to be ongoing.

10 Think globally

In this report we focus primarily on the GDPR (as implemented in the UK by the Data Protection Act 2018). However, CAVs are not static and, in a globalised world, CAVs will be travelling across borders. Therefore, compliance needs to be flexible from country-to-country and the different regimes will need to be considered and complied with. This was recognised by the Inland Transport Committee of UNECE as 31 countries (so far) adopted a resolution to show their commitment to ensuring harmonisation and interoperability of connected vehicles and the Inland Transport Committee adopted a 2030 strategy for sustainable inland transport. [49]

Where the data is personal data, its use has to be balanced against the rights of the individual and ensuring user trust; it is clear that CAVs will never be able to reach their full potential unless users feel they can trust the technology, and the companies, with their data. Lack of trust may lead to customers not inputting data in the first place or, even worse, not buying into the technology at all. Companies will need to consider data protection at the very early stages of CAV development, adopting a user-focused approach to ensure trust is built and maintained. Reviewing and analysing the data and its security will need to be ongoing to ensure that the approach keeps pace with advancing technologies and the developing regulatory regimes.

CHAPTER 3:

Connnectivity and communications

> *"FLOURISH is a pioneering project that captures user needs and expectations of Connected and Autonomous Vehicles to an unprecedented level of detail, building automation, communication and Human Machine Interface technologies and services that are safe and secure, as well as accepted and trusted by older adults".* [50]
>
> **Dr. Wolfgang Schuster, FLOURISH consortium chair**

In its paper 'Industrial Strategy: Building a Britain fit for the future' [51] the Government recognised the need to ensure a robust digital infrastructure to ensure, amongst other things, that the UK is able to achieve its Grand Challenge of becoming *'a world leader in the way people, goods and services move'*. [52] The Industrial Strategy set out the Government's commitment to invest over £1 billion in digital infrastructure including the provision of £176 million for 5G. The Government has reiterated its commitment to investing in digital infrastructure in its 'Future of Mobility: Urban Strategy' paper in which it recognises that the infrastructure will underpin the success of its Future of Mobility Grand Challenge. [53]

KMPG's AVRI highlights the challenges faced by the UK in terms of its digital and physical infrastructure. The AVRI notes that the UK *"lags behind other countries in 4G coverage, global connectivity…"* but goes on to recognise that *"extensive investments are being made in 5G to connect 5G test beds and test tracks"*. [54]

In its 'Digitising European Industry' strategy, the European Commission highlighted the need to ensure a strategic focus to digital communications and in particular identified the priority areas for standardisation as including 5G, data technologies and cyber security. [55] The European Commission noted that this was a *'clear requirement'* for the deployment of CAVs.

In response to this need, the European Commission has recently published a final draft of its delegated regulation on the deployment and use of cooperative intelligent transport systems (**C-ITS**) (the "**Regulation**"). [56]

The focus of C-ITS is on communication between intelligent transport systems. This communication may be vehicle-to-vehicle, vehicle-to-infrastructure or with other C-ITS systems. The Regulation is designed to set out the minimal legal requirements for the interoperability of C-ITS to enable large-scale deployment of systems and services with effect from this year. It is focused on services that will be deployment in the near future.

In assessing the need for the European Commission to take action, the Regulation acknowledges that there is already a move towards large-scale deployment of C-ITS services and that whilst there is some industry-led standardisation, it is voluntary and does not assure compatibility of C-ITS solutions across the European Union.

In the Explanatory Memorandum to the Regulation, the European Commission sets out the need to ensure that where the exchange of messages between C-ITS stations involves the transmission of personal data, stakeholders operating C-ITS either as a data controller or data processor will need to comply with the GDPR [57] and the e-Privacy Directive. [58]

Cooperative Intelligent Transport Systems

> *"In many respects today's vehicles are already connected devices. However, in the very near future they will also interact directly with each other and with the road infrastructure. This interaction is the domain of Cooperative Intelligent Transport Systems (C-ITS)… This cooperative element – enabled by digital connectivity – is expected to significantly improve road safety, traffic efficiency and comfort of driving…"* [59]

[50] FLOURISH mid-project trials report, 23 October 2018.

[51] HM Government 'Industrial Strategy: Building a Britain fir for the future' (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf)

[52] Ibid, page 10

[53] Department for Transport 'Future of Mobility: Urban Strategy – Moving Britain Ahead' published March 2019 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/786654/future-of-mobility-strategy.pdf)

[54] KPMG '2019 Autonomous Vehicles Readiness Index – Assessing countries' preparedness for autonomous vehicles' (https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf)

[55] European Commission 'Digitising European Industry – Reaping the full benefits of a Digital Single Market' COM(2016) (https://eur-lex.europa.eu/legal-content/EN TXT/?qid =1479300554594&uri=CELEX:52016DC0180)

Over the course of the FLOURISH project, partners have been working to research, develop and trial relation and cyber-resilient communications for vehicle-to-infrastructure. The focus of the three car trials undertaken as part of the FLOURISH project has been to examine the necessary conditions for implementing a CAV communications network with a focus on vehicle to roadside infrastructure. Within the range of C-ITS, the car trials explored the application of wireless short range communications (ITS G-5) which is dedicated to automotive intelligent transport systems. [60]

C-ITS will not necessarily replace traditional cellular (e.g. 4G, 5G) communications for CAVs. The two technologies will have differing practical applications and the choice of technology will likely be determined by the market depending on the particular use-case. [61]

The FLOURISH car trials have focused on exploring the deployment of C-ITS for CAVs. In a demonstration of the value of the FLOURISH project to achieving the UK's Future of Mobility Grand Challenge, the output of the trials includes the first complete data set to record the whole set of ITS-G5 network interactions; whilst this data set is incredibly important to the project, it has also been made publically available to ensure future network comparisons. [62]

The car trials have:

- demonstrated the packet delivery ratio (PDR) which is the ratio of messages transmitted to messages received. This is important for the transmission of safety-critical message sets; [63]
- demonstrated the viability of operating an ITS-G5 system for CAVs supporting the efforts of stakeholders in working towards achieving the UK's Future of Mobility Grand Challenge; [64]
- delivered a data set which can be utilised by experts in cyber security to train anomaly detect systems, for example, by measuring the compatibility between a maliciously broadcast co-operative awareness message (CAM) and a road-side-unit capable of measuring the received signal strength indicator (RSSI) of the malicious CAM, which will be based on geographic location of the malicious CAM. [65]

As we set out in Chapter 1 of our Report, carefully considering how new and evolving communications technologies, such as C-ITS, can be integrated into the transport system will be vital for underpinning the security and trust in the CAV ecosystem.

[56] Commission Delegated Regulation (EU) of 13 March 2019 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the deployment and operational use of cooperative intelligent transport systems C(2019) 1789 final.

[57] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[58] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[59] European Commission 'A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility' COM(2016) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016DC0766)

[60] ETSI 'Automotive Intelligent Transport Systems' (https://www.etsi.org/technologies/automotive-intelligent-transport?highlight=WyJpdHMtZzUiXQ==)

[61] Transport Technology Forum 'Local and Cellular Communications: A guide to help policy development' March 2017 (http://its-uk.org.uk/wp-content/uploads/2017/04/A-comparison-of-ITSG5-with-cellular-comms-policy-implications.pdf)

[62] I Mavromatis, A Tassi and R Piechocki 'Operating ITS-G5 DRSC over Unlicensed Bans: A City-Scale Performance Evaluation' (April 2019)

[63] See 46

[64] See 46

[65] I Mavromatis, A Tassi and R Piechocki 'A Dataset of Full-Stack ITS-G5 DSRC Communications over Licensed and Unlicensed Bands Using a Large-Scale Urban Testbed' (April 2019)

CHAPTER 4

Recommendations and conclusions

Recommendations

1. Industry stakeholders to collaborate to begin to determine a 'data map' for the CAV ecosystem which can be used industry-wide to support effective data management.
2. The government should continue to invest in cyber security, in particular in relation to cyber security for CAVs.
3. The government should continue to invest in the development of CAV technology and cyber security, including through the continued funding of test facilities, and industry-led research and development projects.
4. The UK should continue to maintain a global outlook in researching and developing CAVs to ensure that the UK's products and services are able to service a global market.

Conclusions

During the FLOURISH project we have seen an increasing spotlight on the issues of data and cyber security. Data is the new fuel and one for which all stakeholders, to varying degrees, will be responsible.

We continue to recognise, welcome and support the considerable progress that is being made in these areas by government, regulators, industry bodies and stakeholders. We are particularly pleased to be a part of these discussions supporting the CAV ecosystem with our respective in-depth knowledge and understanding of data and cyber security from both an insurance and legal perspective, and continue to be encouraged by the pace of progress.

There is still much more work to be done in the UK if we are to see fully autonomous vehicles on UK roads by 2021. Data and cyber security considerations will remain a fundamental component of the success of the CAV ecosystem.

We would like to take this opportunity to give our thanks to our fellow FLOURISH consortium members – both the organisations and the people involved in the project – for their knowledge, commitment to the project and overall, to furthering the work to develop products and services that maximise the benefits of CAVs for all.

Burges Salmon and AXA remain committed to working towards achieving data and cyber security frameworks which support the successful adoption of CAVs and which are properly balanced against individuals' interests.

flourish
EMPOWERMENT THROUGH TRUSTED SECURE MOBILITY

About the authors

Burges Salmon

Burges Salmon is an independent UK law firm. Our transport lawyers have unrivalled expertise in the transport sector across all modes. We combine that expertise with cutting-edge legal and regulatory experience and thought leadership though our Transport Technology and Intelligent Mobility practice. Our work includes feasibility, research and development and commercialisation projects and working with innovative mobility solutions providers. On Connected and Autonomous Vehicles, we lead on critical analysis and thinking on legal and regulatory reform, grounded in actual testing experience through our involvement in four government-funded CAV projects: VENTURER, FLOURISH, CAPRI and ROBOPILOT.

www.burges-salmon.com

- Chris Jackson, Partner, Transport, chris.jackson@burges-salmon.com
- Lucy Pegler, Senior Associate, Technology and Transport, lucy.pegler@burges-salmon.com

AXA

AXA UK is part of the AXA Group, the largest insurance brand in the world and the largest insurer by revenue. We operate across 61 countries, with 105 million customers worldwide. AXA is committed to finding and developing ways to make our roads safer, and it may sound dramatic but as the cause of over 90% of road traffic accidents is driver error, we believe the way to achieve this is by removing the driver from the driving seat.

AXA has been heavily involved in the field of autonomous cars since 2014, recognising the positive societal impact the technology could have, and is currently part of five different trials across the country which are testing these vehicles ahead of their introduction onto British roads.

www.axa.co.uk

- David Williams, Managing Director, Underwriting & Technical Services, AXA Insurance, david.j.williams@axa-insurance.co.uk
- Sophie Bonnel, Senior Public Affairs Executive, sophie.bonnel@axa-uk.co.uk
- Jonathon Murphy, Public Affairs Executive, jonathon.murphy@axa-uk.co.uk

AXA

Burges Salmon

flourish

EMPOWERMENT THROUGH **TRUSTED** SECURE MOBILITY

Insurance & Legal Report

2019