Insurance & Legal Report

2018

flourish

EMPOWERMENT THROUGH TRUSTED SECURE MOBILITY

M4(E)
London
Bristol(C)
(M32)
M4(W)
S. WALES
Chepstow
(M48)
The SOUTH WEST
Bristol(W) &
M5
15

Contents

About FLOURISH 02

Joint Foreword 03

Chapter 1: Cyber Security and CAV Technology 04

1. Security Challenges

2. The UK

3. The Key Principles of Vehicle and Cyber Security for Connected and Autonomous Vehicles

4. The Developing Legal Landscape

- GDPR, DPA 2018 & NIS Directive
- NIS Regulations
- The Automated and Electric Vehicles Act 2018

Chapter 2: Data and the User 14

Chapter 3: Lawfully Processing Data 16

Chapter 4: Conclusion 22

Recommendations 23

About the Authors 24

flourish

EMPOWERMENT THROUGH **TRUSTED** SECURE MOBILITY

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

Central to FLOURISH is a user-based approach; one which seeks to examine and understand user demands and expectations to ensure that the full potential of Connected and Autonomous Vehicles is unlocked.

At the time of writing this report, the General Data Protection Regulation (GDPR) has been in effect for nearly five months. Why is this relevant? We know that CAVs will generate data on an unprecedented scale. Whilst not all data generated will be personal data, we know that users rightly expect that their data is used in a way that is fair, open and transparent and, importantly, in a way that is secure.

GDPR has re-shaped and updated organisations' approach to the use of personal data. Importantly, it has also allowed an opportunity for individuals to learn about their rights in respect of their data. It is the framework upon which we base discussions about how we can successfully balance the need to ensure that user personal data is used correctly against the need to enable innovation. And in this sense, law and insurance is an enabler. As we said in our year 1 report, law and insurance should unlock opportunities whilst protecting people by balancing the collective good with individual requirements; providing clear accountabilities and risk allocation.

This report focuses on developments in the past year in cyber security and data protection. It starts to explore some of the key concepts of GDPR and aims to begin to shape a framework for the inevitable but crucially important discussions around personal data. Additionally, this report explores the importance of understanding the data flows in the CAV ecosystem – not just for personal data but for all data. It is fundamentally important that we start to address some of the core questions around the availability of data and access rights to that data. In Chapter Four this report identifies a number of recommendations pertaining to data, cybersecurity and investment which we hope, as with our recommendations in our year 1 report, continue to contribute to the evolution of CAVs.

We would like to thank all of our FLOURISH partners in particular Traverse for their insightful user workshops. We would also like to thank our colleagues for their work on this report in particular Lucy Pegler and Zoe Gillingham at Burges Salmon and Sophie Bonnel at AXA.

October 2018

Chris Jackson
Head of Transport Sector
Burges Salmon LLP

David Williams
Technical Director
AXA

CHAPTER ONE: Cyber Security and CAV Technology

In our year 1 report[1] we considered the advent of CAVs and the importance of cyber security. Since then we have seen many high profile cyber security incidents, the UK government has announced that it wants to see fully autonomous vehicles on UK roads by 2021[2] and analysts predict that by 2026, the global autonomous vehicle market will be valued at more than $500 billion[3] - the protection of CAVs and the CAV ecosystem remains as important as ever.

Security Challenges

The European Union Agency for Network and Information Security (ENISA) has identified that the security challenges in autonomous systems such as CAVs primarily emerge from:

- resilience requirements;
- trust requirements; and
- integrity requirements.[4]

ENISA recognises that trust relationships are particularly important to CAVs given that they will *"probably be critically dependent on information exchanges with the outside world".*

ENISA predicts that autonomous systems will require novel approaches in security given that they belong to the Internet of Things (IoT) environment. The protection of deployments within the IoT depends upon the protection of all systems involved, the devices themselves, cloud backed services and maintenance and diagnostic tools to name a few.[5]
Risks are related to cyber security threats and come from many areas – lack of integration between information technology and operational technology, insider threats, vulnerabilities in mobile applications, outdated software and lack of information sharing.[6]

[1] FLOURISH, Insurance and Legal Report (2017) http://www.flourishmobility.com/storage/app/media/publication/J381379_Brochure_Flourish%20Report_V14_SPREADS.pdf
[2] HM Government, Industrial Strategy Building a Britain fit for the future (November 2017) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf
[3] Allied Market Research, Global Autonomous Vehicle Market Opportunities and Forecasts 2019 – 2026 (May 2018) https://www.alliedmarketresearch.com/autonomous-vehicle-market
[4] ENISA, Looking into the crystal ball A report on emerging technologies and security challenges (January 2018) https://www.enisa.europa.eu/publications/looking-into-the-crystal-ball
[5] ENISA, Baseline Security Recommendations for IoT (November 2017) https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[6] ENISA, Taking stock of information security training needs in critical sectors (December 2017) https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors

According to ENISA[7], 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 is the most frequently encountered cyber threat and that increasingly there is no need for user interaction to install the threat,[8] i.e. users don't need to 'click' to open a URL, the malware simply installs itself. For example, a CAV could receive a software update from a seemingly legitimate source which then automatically infects the CAV system with software that limits functionality. The main concern in the CAV ecosystem is that one compromised vehicle could spread the malware throughout the system through the routine data sharing that will take place.

Ransomware – this is a type of malicious software that usually involves blocking access to a computer system until the attackers are paid ransom money. The NHS WannaCry attack is an example of a ransomware attack.

Denial of service (DoS) – a DoS attack occurs where attackers flood IT systems with information which then prevents legitimate users from accessing the system. For example, flooding a website with access requests to the point that the site crashes. A volumetric attack like this is often a much less sophisticated but equally successful way of an attacker disrupting systems.

Data breaches – this term describes the result of an effective cyberattack rather than a type of attack of itself. [9] A data breach is a situation where data has been lost or stolen somehow and so is only usually discovered after it has occurred, sometimes not until years later. It is estimated that there are far more data breach incidents than those actually reported or detected. For the CAV ecosystem, it will be essential to secure data to maintain the integrity of the system.

Cyber espionage – this is defined as *"the use of the use of computer networks to gain illicit access to confidential information, typically that held by a government or other organisation"*. [10] ENISA identifies that attackers are creating new techniques and tools in an attempt to steal intellectual property and secrets.[11]

[7] ENISA, Threat Landscape Report 2017 15 Top Cyber-Threats and Trends (January 2018) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
[8] ENISA, Threat Landscape Report 2017 15 Top Cyber-Threats and Trends (January 2018) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
[9] ENISA, Threat Landscape Report 2017 15 Top Cyber-Threats and Trends (January 2018) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017
[10] Oxford English Dictionary https://en.oxforddictionaries.com/definition/cyberespionage (Accessed September 2018)
[11] ENISA, Threat Landscape Report 2017 15 Top Cyber-Threats and Trends (January 2018) https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

The UK

"As our reliance on technology grows the impact of failure in those systems and the opportunities for those who would seek to compromise our systems and data increase. Responding to this threat and ensuring the safety and security of cyberspace is an essential requirement for a prosperous UK economy."[12]

The UK government recognises the importance of cyber security. In its report, 'Connected and Autonomous Vehicles: The Future?' [13], the House of Lords Science and Technology Committee highlighted the extent to which CAVs will be a target for cyber-attack and set out evidence it had received from stakeholders on the importance of government taking *"a strong coordinating role".* In response to the House of Lords' report, the government stated:

"Through our Industrial Strategy, we are investing jointly with industry in both research and development and the development of testing environments to ensure that the UK remains at the forefront of the development of this technology."[14]

In November 2017, the government published its 'Interim Cyber Security Science & Technology Strategy: Future-proofing cyber security'.[15] In its interim report, the government set out that "as a global industry, the automotive sector requires a consistent, global approach to [cyber security] and [the government] is already working to achieve this" and noted that "the government will provide direction and clear expectation to industry to ensure that vehicles safely communicate with the world around them, including other vehicles and infrastructure". Setting out its steps to achieve this, the government highlighted (amongst other things) that it will:

- work with industry through (a) engagement, (b) sponsoring an industry-led automotive information exchange of threat and vulnerability intelligence and solutions, and (c) support of industry bodies including insurers to develop a maturity assessment framework which could enable the insurance industry to perform cyber risk assessments on automotive systems;
- work with international partners; and
- provide guidance setting out what government thinks good cyber security looks like and developing an automotive specific framework for security assessment.

The UK's Industrial Strategy[16]

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 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.

[12] Department for Digital, Culture, Media & Sport (https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018)
[13] House of Lords Science and Technology Select Committee report "Connected and Autonomous Vehicles: The future?" published March 2017 https://www.parliament.uk/documents/lords-committees/science-technology/autonomous-vehicles/HMG-response-connected-autonomous-vehicles-report.pdf[14]
[14] Department for Transport Department for Business, Energy, Innovation and Skills Response to House of Lords Science and Technology Select Committee report "Connected and Autonomous Vehicles: The future?" 2nd Report of Session 2016–17 (October 2017) https://www.parliament.uk/documents/lords-committees/science-technology autonomous-vehicles/HMG-response-connected-autonomous-vehicles-report.pdf
[15] Cabinet Office 'Interim Cyber Security Science & Technology Strategy: future-proofing cyber security' https://assets.publishing.service.gov.uk/government/uploads/system uploads/attachment_data/file/663181/Embargoed_National_Cyber_Science_and_Technology_Strategy_FINALpdf.pdf
[16] HM Government, Industrial Strategy – Building a Britain fit for the future (27 November 2017) https://assets.publishing.service.gov.uk/government/uploads/system/uploads attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf

THE STUDENTS'
UNION
AT UWE
CATAPULT
flourish

The Key Principles of Vehicle and Cyber Security for Connected and Autonomous Vehicles

To assess the cybersecurity risks posed by CAVs, it is vital to consider the entire ecosystem - the underlying operation of CAVs, the cloud services they connect with, maintenance systems and any systems the vehicles may 'speak' to (for example, smart roads and traffic updates). The CAV ecosystem is both interconnected and interdependent. Whilst the development of CAV technology is progressing at an exciting pace, there is a fundamental need to develop baseline security requirements across the ecosystem which allow for the management of risk but with room for innovation. Cyber security will become as important as traditional service and maintenance and product assuredness.

In August 2017 the government announced its '*Key Principles of Vehicle and Cyber Security for Connected and Autonomous Vehicles'* (developed together with the Centre for Protection of National Infrastructure).[17] The principles are not legally binding but are a step in the right direction towards promoting cyber security for CAVs. The government has recognised that:

"[it is] essential that all parties involved in the manufacturing supply chain, from designers and engineers, to retailers and senior level executives, are provided with a consistent set of guidelines that support this global industry". [18]

In our year 1 report,[19] we made a number of recommendations in terms of cyber security that we felt would be key to unlocking the societal benefits of CAV technology. We are pleased to see that many of the issues we identified have been captured in the principles. Throughout, the principles hint at data protection requirements proving again that cyber security for CAVs is not just about protecting the users' physical environment but also about protecting their personal data and the commercially sensitive data that will no doubt be generated. We set out a summary of the principles below – the key message is that organisations operating in the CAV ecosystem should collaborate to know the risks and embed security throughout the entire lifecycle of CAV technology. We welcome this recommendation and importantly the work being done by the FLOURISH project to achieve this.

Principle 1: Organisational security is owned, governed and promoted at board level.

Accountability is a key theme of Principle 1. Security must be aligned with an organisation's broader mission and objectives and awareness training must be provided to ensure a 'culture of security'. Importantly for CAV development, Principle 1 promotes 'security by design' whereby all aspects of security, including cyber, must be integrated into the product and development service.

Principle 2: Security risks are assessed and managed appropriately and proportionately, including those specific to the supply chain.

Engineering practices must be used to mitigate current and relevant security threats and organisations are expected to understand what these threats are. Principle 2 encourages collaboration to enhance awareness and promotes response planning and the development of procedures that appropriately detect and prioritise risks.

Principle 3: Organisations need product aftercare and incident response to ensure systems are secure over their lifetime.

Lifetime system security is a key consideration in the CAV ecosystem. Principle 3 focusses on organisations:

- planning to maintain security over the life of the system, including after sales support;
- having adequate incident response plans to return affected systems to a safe and secure state;
- having active programmes to identify critical vulnerabilities; and
- ensuring that systems can support adequate data forensics such that the cause of a cyber incident (or other incident) can be determined.

These elements will all be key to user acceptance in the CAV ecosystem. For developers and insurers, it presents the crucial question - who will be responsible for what? This question has since, at least in part, been answered by the Automated and Electric Vehicles Act (this is discussed further in this report).

Principle 4: All organisations, including sub-contractors, suppliers and potential 3rd parties, work together to enhance the security of the system.

Under Principle 4, organisations are expected to:

- collaborate to enhance security;
- provide assurance of their security processes and products;
- be able to ascertain and validate the authenticity and origin of their supplies;
- plan together how systems will interact safely and securely with external devices, ecosystems and services (including maintenance); and
- manage external factors. Plus, where external factors are critical to automated functions, organisations must employ secondary measures to account for this.

Principle 4 suggests that independent validation or certification may assist with some of these elements.

[17] HM Government, The Key Principles of Cyber Security for Connected and Automated Vehicles (August 2017) https://assets.publishing.service.gov.uk/government/uploads system/uploads/attachment_data/file/661135/cyber-security-connected-automated-vehicles-key-principles.pdf
[18] https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles
[19] FLOURISH, Insurance and Legal Report (2017) http://www.flourishmobility.com/storage/app/media/publication/J381379_Brochure_Flourish%20Report_V14_SPREADS.pdf

Certainly the values underlying Principle 4 are key for user acceptance in the CAV ecosystem. With so many different players, collaboration will be a crucial element of success. Moreover, on a fundamental level, the CAV ecosystem cannot function without it.

Principle 5: Systems are designed using a defence-in-depth approach.

Under Principle 5 the security of a system must not rely on one single point of failure. Security must employ 'defence-in-depth' techniques which involves complimentary layers of security measures such as trust layers and monitoring. In addition, design controls must be in place across 'trust boundaries' where data is shared, e.g. use of encryption measures and minimising the use of shared data storage. Such requirements are likely to be most familiar to stakeholders in the technology and tech-development industries. Effectively communicating the use of personal data to individuals plays an important role in fostering trust. Recent figures published by the ICO[20] highlight that only 34% of people surveyed have trust and confidence in organisations which store and use their personal data. Whilst this is a welcome improvement on the figures from 2016, it supports the clear need to ensure openness and transparency with individuals to ensure that they understand how CAVs and those stakeholders in the ecosystem will use their data and the benefits they will receive from sharing their personal data which will inevitably contribute towards user acceptance of CAV technology.

Principle 6: The security of all software is managed throughout its lifetime.

Principle 6, as with Principle 3, promotes the concept of a lifetime of security. Principle 6 sets out that:

- organisations should adopt coding practices that are secure and manage risk from known and unknown software vulnerabilities;
- it must be possible to ascertain the status of all software;
- it must be possible to safely and securely update software; and
- peer reviewed code, plus sharing of code, must be used where possible.

Of key significance is the element of the unknown. How do you future proof the future?

Principle 7: The storage and transmission of data is secure and can be controlled.

There are three elements to Principle 7 – data must be sufficiently secure when stored and transmitted, personally identifiable data must be managed securely both in storage and transmission, and users must be able to delete sensitive data held on connected systems. This closely mirrors data protection requirements under the GDPR [21] (and DPA 2018) demonstrating that they are inextricably linked to the concept of security in the CAV ecosystem.

As the CAV ecosystem emerges, we can expect to see further guidance on the application of data protection requirements. This will aid risk allocation and thus further the concept of accountability which was introduced in Principle 1 and is a fundamental concept of GDPR.

Principle 8: The system is designed to be resilient to attacks and respond appropriately when its defences or sensors fail.

Systems must be both resilient and fail safe should safety critical functions be attacked or stop working. And, if non-safety critical functions fail, systems must be able to respond appropriately. Furthermore, external and internal interfaces must be able to withstand attack from corrupt or malicious data or commands by remaining available for their primary use.

[20] The Information Commissioner's Office, the UK's independent data protection supervisory authority.
[21] 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.

The Developing Legal Landscape

GDPR, DPA 2018 & NIS Directive

Personal Data: Information relating to a natural, living person who can be identified (directly or indirectly) from that information or from that information plus other available information. For example, name, location data and online identifiers (such as cookies). In the CAV ecosystem, there will be an abundance of personal data.

GDPR - 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)

As anticipated, GDPR and the UK's Data Protection Act 2018 (DPA 2018) entered into force in May 2018. Whilst most of the narrative was around protection of personal data, cyber security is unquestionably a key consideration given that GDPR (and therefore the DPA 2018) requires that organisations ensure appropriate organisational and technical security measures to protect personal data.

Examples of such measures include the pseudonymisation and encryption of data but organisations must also implement measures which maintain the confidentiality, integrity and availability of data, restore access to data following a security incident and have adequate processes to test, assess and evaluate systems that have been implemented.

With limited further guidance as to what might constitute an appropriate organisational or technical security measure, organisations must work to both identify and implement adequate measures considering the following:

- state of the art security measures;
- the costs of implementation;
- the nature of the data being used, the scope and context of its use and the purpose of its use; and
- the risks of the data being compromised and the effect of such on individuals.

As a minimum, players in the CAV ecosystem will likely be expected to have robust testing and back-up regimes in place to regularly audit the suitability of their chosen security measures.

Q&A - The Data Protection Act 2018

What is the DPA 2018?

The DPA 2018 is the UK's third generation of data protection law.[22] It regulates the use of information relating to individuals and makes provisions in connection with the function of the Information Commissioner's Office (ICO), the UK's data protection supervisory authority. The DPA 2018 replaces and repeals it forerunner, the Data Protection Act 1998.

What is its purpose?

The purpose of the DPA 2018 is to update and modernise data protection law in the UK.[23] It aims to make data protection law suitable for the digital age, empower individuals in respect of their own data, support UK businesses and organisations and ensure that the UK is prepared for the post-Brexit future,[24] i.e. ensuring that EU and UK data protection laws are aligned.

"In the digital world strong cyber security and data protection go hand in hand. The 2018 Act is a key component of our work to secure personal information online." Matt Hancock MP, former Secretary of State for the Department for Digital, Culture, Media and Sport.[25]

How does the DPA 2018 interact with GDPR?

The DPA 2018 implements GDPR standards and provides clarity on definitions used in GDPR.[26] In addition, the DPA 2018 includes detail of how GDPR will apply in the limited instances that GDPR allows the UK (and other EU member states) to dictate such provisions (e.g. in academic research, financial services and child protection). As well as covering GDPR requirements, the DPA 2018 also covers general data, law enforcement data, immigration and national security data.[27,28] Consequently, the ICO recommends that GDPR and the DPA 2018 are read side-by-side.[29]

Security Incidents

There is *"…a need to improve the security of network and information systems across the UK, with a particular focus on essential services which if disrupted, could potentially cause significant damage to the economy, society and individuals' welfare."*[30] National Cyber Security Centre

[22] ICO, Data Protection Act 2018 https://ico.org.uk/for-organisations/data-protection-act-2018/ (Accessed September 2018)
[23] ICO, Data Protection Act 2018 https://ico.org.uk/for-organisations/data-protection-act-2018/ (Accessed September 2018)
[24] Department for Digital, Culture Media & Sport, Data Protection Act 2018 Factsheet - Overview https://assets.publishing.service.gov.uk/government/uploads/system/uploads attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf (25 May 2018)
[25] Department for Digital, Culture Media & Sport, Data Protection Act 2018 Factsheet - Overview https://assets.publishing.service.gov.uk/government/uploads/system/uploads attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf (25 May 2018)
[26] Department for Digital, Culture Media & Sport, Data Protection Act 2018 Factsheet - Overview https://assets.publishing.service.gov.uk/government/uploads/system/uploads attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf (25 May 2018)
[27] ICO, Data Protection Act 2018 https://ico.org.uk/for-organisations/data-protection-act-2018/ (Accessed September 2018)
[28] Department for Digital, Culture Media & Sport, Data Protection Act 2018 Factsheet - Overview https://assets.publishing.service.gov.uk/government/uploads/system/uploads attachment_data/file/711162/2018-05-23_Factsheet_1_-_Act_overview.pdf (25 May 2018)
[29] ICO, Data Protection Act 2018 https://ico.org.uk/for-organisations/data-protection-act-2018/ (Accessed September 2018)
[30] National Cyber Security Centre, Introduction to the NIS Directive https://www.ncsc.gov.uk/guidance/introduction-nis-directive (28 January 2018) (Accessed September 2018)

Together, GDPR and the European Network and Information Systems Directive **(NIS Directive)** set a baseline for cyber security across the EU. Whilst GDPR focusses on the protection of personal data, the NIS Directive is concerned with preventing, handling and responding to security incidents affecting network and information systems.

Introduced in 2016, the NIS Directive aimed to improve cyber security capabilities across the EU as a way of improving the overall resilience of network and information systems. Under the NIS Directive 'operators of essential services' OES will need to increase the security of network and information systems.

The NIS Directive was implemented into UK law, also in May 2018, as the NIS Regulations (NIS Regulations). The NIS Regulations are part of the government's National Cyber Security Strategy.[31]

NIS Regulations

The government anticipates that the NIS Regulations will better prepare operators in a number of industries, including transport, to deal with the increasing number of cyber threats anticipated.[32]

Under the NIS Regulations, the government must designate and publish a strategy to provide strategic objectives on the security of network and information systems across the UK. The NIS National Strategy is yet to be released.[33]

As anticipated, through the NIS Regulations, certain road authorities have been identified as OESs. Whilst this means that for now CAV operators have not been identified as OESs, they will likely still have to comply with the NIS Regulations in order to access the roadways. Furthermore, they may be designated as an OES in the future.[34]

An OES must take "appropriate and proportionate technical and organisational measures" to manage security risks of the network and information systems on which their essential service relies and must have regard to relevant guidance produced by the competent authority when doing so.[35] Overall the ICO is the competent authority for relevant digital service providers. Specifically for road transport, the competent authority is the Secretary of State for Transport (England and Wales), the Scottish Ministers (Scotland) and the Department of Finance (Northern Ireland).[36]

Fines of up to £17million may be imposed on an OES for non-compliance issues.

The Automated and Electric Vehicles Act 2018

The Automated and Electric Vehicles Act became law on 19 July 2018. Crucially, as regards automated vehicles, the Act maintains the proposed "single insurer model" under which drivers will buy an automated vehicle policy which covers accidents regardless of whether or not the car was being driven by the driver or autonomously at the time. Following consultation, this was the much preferred model as it offered drivers and all road-users the greatest insurance certainty and the most efficient route for liability recovery.[37]

"The unlocking of this perceived insurance issue around the use of CAVs through the single insurer model is good for the UK CAV sector, good for drivers and good for all road-users. It also reinforces the importance of insurers in facilitating the growth of CAV development and deployment and underlines why we work closely with market leaders such as AXA on a number of CAV projects" – Chris Jackson[38]

The Cyber Breaches Survey 2018

The Cyber Breaches Survey 2018 undertaken by the Department for Culture, Media and Sport as part of the Government's National Cyber Security Programme reveals some interesting insights about the attitudes of businesses to cyber security.

74% of businesses say that cyber security is a high priority for their organisation's senior management.

The number of businesses saying cyber security is a low priority has fallen since 2016 from **30%** to **24%.**

The average investment in cyber security in the last financial year for a business operating in the transport sector was **£6,570.** This is in comparison to an average spend of **£17,900** in the finance and insurance sector

47% of businesses invest in cyber security to protect the data of customers.

[31] Department for Digital, Culture, Media & Sport (https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018) (Accessed 20 July 2018)
[32] Department for Digital, Culture, Media & Sport (https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018) (Accessed 20 July 2018)
[33] Regulation 2(1) NIS Regulations.
[34] Under Regulation 8(3) of the NIS Regulations, the Secretary of State can designate an operator of essential services.
[35] Regulation 10, NIS Regulations.
[36] Regulation 4, NIS Regulations.
[37] https://www.burges-salmon.com/news-and-insight/legal-updates/government-introduces-the-automated-and-electric-vehicles-bill/
[38] https://www.burges-salmon.com/news-and-insight/legal-updates/government-introduces-the-automated-and-electric-vehicles-bill/[33] Regulation 2(1) NIS Regulations.

CATAPULT | flourish
Vehicle trials
in progress

CHAPTER TWO: Data and the User

"Personal data has become the currency by which society does business, but advances in technology should not mean organisations racing ahead of people's rights. Individuals should be the ones in control and organisations must demonstrate their accountability to the public."[39]

The successful functioning of the CAV ecosystem will rely upon data sharing between all players – to and from user and CAV, manufacturer to CAV, CAV to CAV and between many other stakeholders. Data will act as the new fuel.

User engagement and trust will be pivotal to the successful deployment of CAVs. Developing a robust framework for the sharing of data that achieves regulatory compliance in a manner that enables the ecosystem to function is hugely important to this, but developing a framework which is understood and trusted by users is key.

"Roads help us navigate to a place; data helps us navigate to a decision."[40]

A recent report by the Open Data Institute **(ODI)** highlighted the value and importance of data in the transport sector. The report explored the tension between how the law defines personal data and how individuals define personal data.

The ODI highlights that individuals define personal data much more broadly taking into account information such as place of work, personal characteristics and information about family members. Consequently, whilst the legal definition sets some specific parameters around the classification of personal data, the 'human' definition is often much more extensive.[41] With this distinction in mind and noting the vast amounts of data collected about individuals when they make a journey, the ODI considers that journey data is personal data.

The distinction between the legal and human definition of personal data is an important one to understand in the context of developing user trust. Research by FLOURISH partner, Traverse,[42] reinforces the need for clarity and communication on what is personal data within the CAV ecosystem. Crucially Traverse's report also highlights the need for clear and effective communication with users. Traverse reports that "a lack of trust in data protection laws and disregard of consent were felt to be worrying for many". Key for participants in Traverse's workshops was clarity over how their data would be used and who it would be shared with; highlighting that participants want to retain control of their data whilst acknowledging that there would need to be a degree of data sharing to enable the effective operation of CAVs.

Trust and the CAV ecosystem

"The FLOURISH project will help develop innovative new tools to improve the understanding of user needs and expectations of connected and autonomous vehicles and includes Age UK as a member of the consortia."[43] Department for Business, Energy, Innovation and Skills.

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.

As part of its report, the ODI surveyed UK consumer attitudes to sharing personal data. The survey found that trust was a key factor in data sharing:

- if an organisation is known and trusted by a consumer, they are more likely to share their data with that organisation;
- 94% of consumers said trust was an important factor in deciding to share personal data;
- 64% of consumers would share personal data with an organisation they know, compared to 36% of consumers who would share with an organisation they did not know.

The ODI report identified that many organisations in the transport sector recognise the need to share data to support the sector in a way that is secure and which protects individuals. This reflects the Information Commissioner's own view that: "the public should be and is at the heart of everything we do".[44] It is also reflective of GDPR which puts people at the forefront and aims to give them control of their own data.

[39] Elizabeth Denham, Information Commissioner, 'Organisations must continue to improve transparency and accountability as ICO survey shows most UK citizens still don't trust organisations with their data' (https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/organisations-must-continue-to-improve-transparency-and-accountability/) 6 September 2018

[40] Open Data Institute 'Personal data in transport: exploring a framework for the future' 2018[36] Regulation 4, NIS Regulations.

[41] The ODI report adopts the human definition of 'personal data' explaining that "while we will always need strong regulation, it is ultimately people who choose whether or not to trust a business with personal data about them" (page 7).

[42] Traverse Group 'Public and Stakeholder research: interim report' May 2018.

[43] Department for Transport Department for Business, Energy, Innovation and Skills Response to House of Lords Science and Technology Select Committee report "Connected and Autonomous Vehicles: The future?"

[44] Elizabeth Denham, Information Commissioner, in a speech delivered at the Data Protection Practitioners' Conference 2018, 9 April 2018.

In addition to trust, research has demonstrated that individuals are more willing to share data when there are benefits both at an individual and collective level. This is supported by the findings of a report by McKinsey which identified that in 2016, 71% of drivers surveyed share their data in exchange for tangible benefits (for example free apps usage or free content but in the future, these benefits could include reduced insurance costs, increased time).[45] This is reflective of the mood as we move towards data as a currency, with a value that allows it to be traded by individuals with organisations in exchange for benefits. It also highlights the importance of communicating with individuals about how their data is being used and the benefits associated with such use.

Establishing trust - why is it important to get this right?

Research commissioned by the Transport Systems Catapult in 2014[46] estimated that by 2025, the value of data to the intelligent transport market will be approximately £32 billion per year. It is not its monetary value that is important; it is its potential.

In a recent blog post,[47] Transport Systems Catapult CEO Paul Campion, highlighted that "different datasets have different sources and uses" and that the value of data increases when it can be added together with other data to build a bigger, better picture of user habits and journey variables (e.g. routes, speeds, times).

The potential held in data can only be unlocked and optimised if users are happy to share that data. Effectively communicating the use of personal data to individuals plays an important role in fostering trust. Recent figures published by the ICO highlight that only 34% of people surveyed have trust and confidence in organisations which store and use their personal data. Whilst this is a welcome improvement on the figures from 2016, it supports the clear need to ensure openness and transparency with individuals to ensure that they understand how CAVs and those stakeholders in the ecosystem will use their data and the benefits they will receive from sharing their personal data. This will inevitably contribute towards user acceptance of CAV technology.

Whilst GDPR does set out specific requirements in respect of information to be provided to individuals where their data is processed, the obligation for providing this information falls on the data controller. This raises the practical implication about who is the data controller,[48] which will in part depend on the model ultimately adopted in relation to co-ordination of the CAV ecosystem. For example, will one party ultimately take responsibility for the co-ordination of data and the sharing of such data with relevant stakeholders? This is an important question to be borne in mind as the CAV ecosystem evolves.

Data Controller: determines the purposes and means of processing personal data.[49]

Processing: any operation or set of operations which is performed on personal data... such as collection, recording, organisation, structuring storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.[50]

[45] McKinsey 'Car data: paving the way to value-creating mobility – Perspectives on a new automotive business model' 2016 (https://www.mckinsey.com/~/media/McKinsey/Industries Automotive%20and%20Assembly/Our%20Insights/Creating%20value%20from%20car%20data/Creating%20value%20from%20car%20data.ashx)
[46] Transport Systems Catapult 'Intelligent Mobility – Market Breakdown' (https://ts.catapult.org.uk/intelligent-mobility/market-breakdown/).
[47] Transport Systems Catapult, 'Transport data in an insecure world' 16 April 2018 (https://ts.catapult.org.uk/2018/04/16/28488/)
[48] For further discussion on this, refer to FLOURISH Year 1 Insurance and Legal Report.
[49] ICO, Guide to the General Data Protection Regulation (GDPR), 2 August 2018
[50] GDPR, Article 4(2)

CHAPTER THREE: Lawfully Processing Data

In our year 1 report for FLOURISH, we set out our recommendations in relation to the categorisation of data.[51] Compliance with data protection laws should be seen as holistic – it is not a menu to choose from.

In this section of the report we focus on the legal bases for processing personal data under GDPR.

The lawful bases for processing

In order to process personal data – that is in order to do virtually anything with data from which an individual can be identified – a data controller must be able to demonstrate a valid lawful basis.

When considering the application of GDPR, there are two types of data we are primarily concerned with:

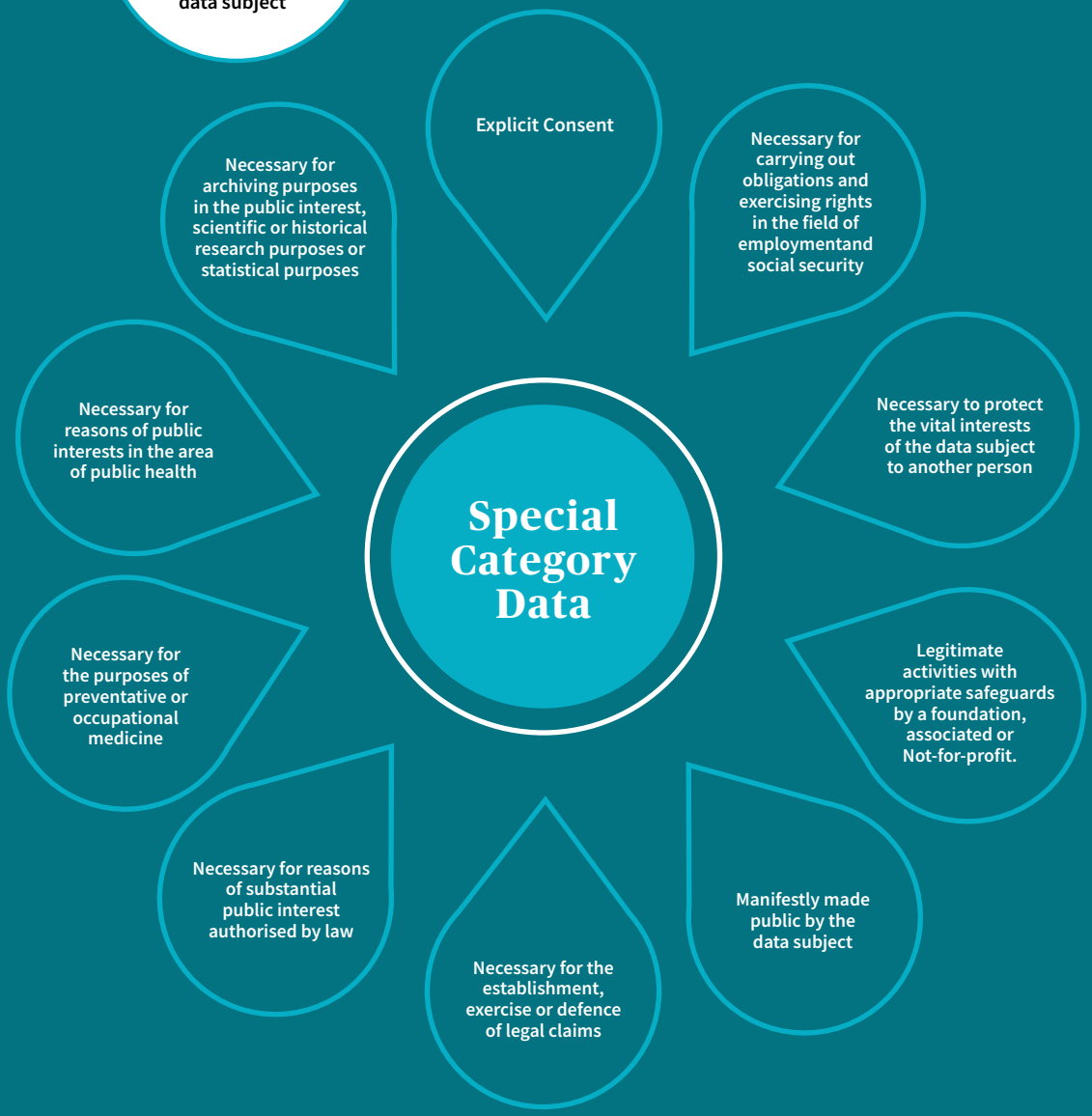
Personal data – any data which relate to a living individual who can be identified from those data or from those data and other information which is in the possession of (or likely to be in the posession of) the controller (e.g. geolocation data, collision data, user habits).

Special category data – any personal data which consist of information relating to racial or ethnic origin, political, religious or philosophical beliefs, trade union membership, physical or mental health/condition genetics or biometrics, sexual life/orientation or the commission (or alleged commission) of any offence or proceedings relating to such.

This is important because when processing special category data, a controller must identify both a lawful basis for the processing of personal data plus an additional lawful basis for the processing of special category data.

[51] FLOURISH Year 1 report – Chapter 3, Data as the new fuel. Article 5(1)(a) GDPR.

Personal Data
Consent
Necessary for the performance of a contract
Necessary for compliance with a legal obligation
Necessary toprotect the vital interests of data subject
Necessary for the performance of a task carried out in the public interest
Necessary for the legitimate interests of the controller or a third party


Special Category Data
Explicit Consent
Necessary for carrying out obligations and exercising rights in the field of employmentand social security
Necessary to protect the vital interests of the data subject to another person
Legitimate activities with appropriate safeguards by a foundation, associated or Not-for-profit.
Manifestly made public by the data subject
Necessary for the establishment, exercise or defence of legal claims
Necessary for reasons of substantial public interest authorised by law
Necessary for the purposes of preventative or occupational medicine
Necessary for reasons of public interests in the area of public health
Necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

Legal Bases for Processing

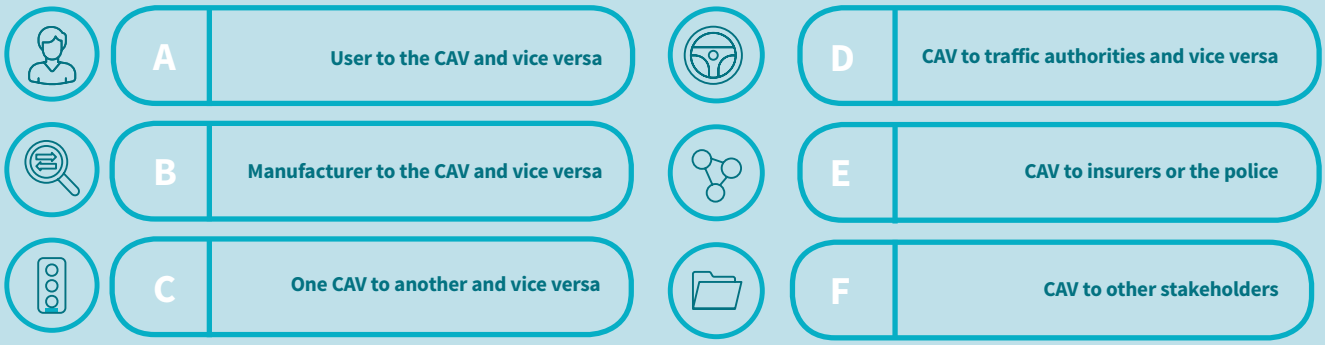
The appropriate lawful bases

Principle 1, GDPR: Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.[52]

GDPR sets outs seven principles which should lie at the heart of any processing of personal data.[53] The first principle of GDPR requires that personal data must be processed lawfully, fairly and in a transparent manner. The ICO explicitly rules out the adoption of a 'one-size-fits-all approach' meaning that the appropriate legal base should be determined based on the context of the specific processing activity.

As an initial step, it will be important to develop an accurate map of the flow of data between the players in the CAV ecosystem. Whilst this is particularly relevant to personal data to ensure open and transparent communication to individuals (as well as regulatory compliance), it will also be key for enabling stakeholders more broadly to understand the data (personal and commercial) that they hold. For the purposes of this section, we focus on personal data.

CAV flow process



For each data flow it will be necessary to consider the appropriate legal base(s) for the processing of that data.

The ICO recommends a number of factors which need to be considered in determining the appropriate legal base:

- the purpose of the processing and intended outcome;
- whether it can reasonably be achieved in a different way;
- whether you have a choice over whether or not to process the data; and
- whether it is being processed by a public authority.

In the CAV ecosystem it is very likely that some processing activities will be done for specified purposes covered by their own lawful base, for example compliance with a legal obligation which applies to the data controller. Where this is the case, establishing the appropriate lawful base will be relatively straightforward. In other instances, the lawful base must be determined through careful assessment.

CAVs and consent

Consent is one of the lawful bases for processing of personal data and special category data. However, consent is not necessarily the answer for CAVs.

Consent is defined as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".*[54]

[52] Article 5(1)(a) GDPR.
[53] ICO, Guide to the General Data Protection Regulation (GDPR), 2 August 2018
[54] Article 4(11) GDPR

The requirements for valid consent:

Distinguishable and in clear and plain language

Consent must be separate from other terms.

Verifiable

The data controller must maintain a record of consent.

Freely given

Individuals must have real choice about whether or not to provide their consent. Consent is presumed not to be freely given if the data subject does not have a genuine free choice or if they are put at a disadvantage by withdrawing or refusing their consent. It must be as easy to withdraw consent as to give it. Public authorities are unlikely to be able to rely on consent for processing activities given that there is considered to be an imbalance of power as between individuals and local authorities.

Given by an affirmative action

A positive action must be taken to signify consent.

Specific and informed

Individuals must be given sufficient information regarding the controller, the purpose(s) of the processing, plus consent cannot be 'bundled' together where different processing activities are taking place, consent must be granular, i.e. individuals must consent to each processing activity rather than a number of processing activities bundled together.

It must be as easy to withdraw consent as to give it[55]

Individuals should be made aware of their right to withdraw consent at the time at which it is first given and on a continuing basis.

For special category data, the bar for consent is raised. Consent must be explicit and that has generally been taken to mean a form of express written statement confirming consent to the processing activities.

The requirements for consent, and in particular that it must be freely given and as easy to withdraw as to give, means that in many cases it will not be the appropriate lawful base for processing of personal data in the CAV ecosystem. Furthermore, if an individual withdraws consent then processing of that data has to stop. This could mean that access to critical personal data is withdrawn. Simply put, the ecosystem cannot effectively function with that level of uncertainty.

If not consent, then what?

It is likely that processing of personal data in the CAV ecosystem will rely on a number of lawful bases. We mentioned that some processing may be done for a specified purpose with its own lawful base. It is also conceivable that some processing may be done on the basis of fulfilling a contractual obligation (i.e. performance of a contract) with an individual or on the controller's legitimate interests in the processing.

[55] Article 7(3) GDPR.

CATAPULT
Transport Systems
flourish

Contract:

Relying on performance of a contract as a lawful basis can be used where the processing of personal data is necessary to (a) fulfil a controller's obligations to that individual, or (b) do something that the individual has asked the controller to do in advance of entering into a contract. Importantly for the CAV ecosystem, this lawful base can only be relied upon as between the individual and data controller.

Legitimate interests:

Relying on legitimate interests as a lawful basis can only be used where individuals would 'reasonably expect' their data to be used in the way that it is being used and with a 'minimal privacy impact', or otherwise where there is another compelling reason to use that individual's data. Although this legal base comes with a degree of flexibility as to application, it is not simple to apply and there are certain tests that must be met in order to rely on it. Those tests require a comprehensive understanding of the specific data processing activities. Whether or not this legal base will be appropriate can only be determined with time and a clear understanding as to how data is to be used and shared between stakeholders in the CAV ecosystem. The work of the FLOURISH project to understand user acceptable will be a key element in understanding how individuals would reasonably expect CAV players to handle their data.

"Every autonomous car will generate the data equivalent of almost 3,000 people"[56]

Not all of this data will be personal data but the projection is astounding and demonstrates the size of the challenge of ensuring that individual rights in respect of their data are maintained. As part of achieving this, a critical step will be mapping the data flows in the CAV ecosystem. In practical terms, this means:

- data considerations need to be at the heart of developing these technologies – this is what FLOURISH is doing. The use of data and in particular personal data cannot be an afterthought once the technology has been developed;
- communication is key and crucially, communication between stakeholders in the ecosystem. The types of data being collected and the uses of that data need to be clear and transparent;
- establishing the appropriate legal bases under GDPR should be a collaborative effort between stakeholders. A clear framework should be adopted which recognises that there will be some 'standard' uses of personal data (for example, by insurers to administer claims, or by manufacturers to enable the operator of CAVs) but maintains the degree of flexibility required to ensure that it responds to technological innovation.

The CAV ecosystem is still in a period of development. The consequence of this is that whilst data protection considerations must be at the forefront of minds, the ecosystem is arguably not at the point of stability which would enable a comprehensive review of data flows or clear identification of the appropriate legal bases for processing. However, it is clear that based on current guidance from the European Data Protection Board and the UK Information Commissioner, consent should not be seen as a 'one-size-fits-all' solution and there will need to be a period of intense and detailed review of data flows. This will ensure that the legal framework developed in relation to the use of personal data in the CAV ecosystem ensures that CAV technologies are appropriately supported whilst balancing this against protecting the fundamental rights and freedoms of individuals in respect of their personal data.

The Law Commissions' Review

"With driving technology advancing at an unprecedented rate, it is important that our laws and regulations keep pace so that the UK can remain one of the world's leaders in this field"

– Jesse Norman MP, Roads Minister

In March 2018, the government announced a detailed three-year review of driving laws to be undertaken by the Law Commission of England and Wales and the Scottish Law Commission. The review will consider a broad range of laws including road traffic legislation and product liability, and will conclude with a proposal for a framework for the future.

The Law Commission has set out that the areas considered in this report – namely data protection and privacy and cyber security – are outside the scope of their review. We expect that in addition to the work of the FLOURISH project, the issue of data protection and privacy will be explored in time by the ICO together with industry.

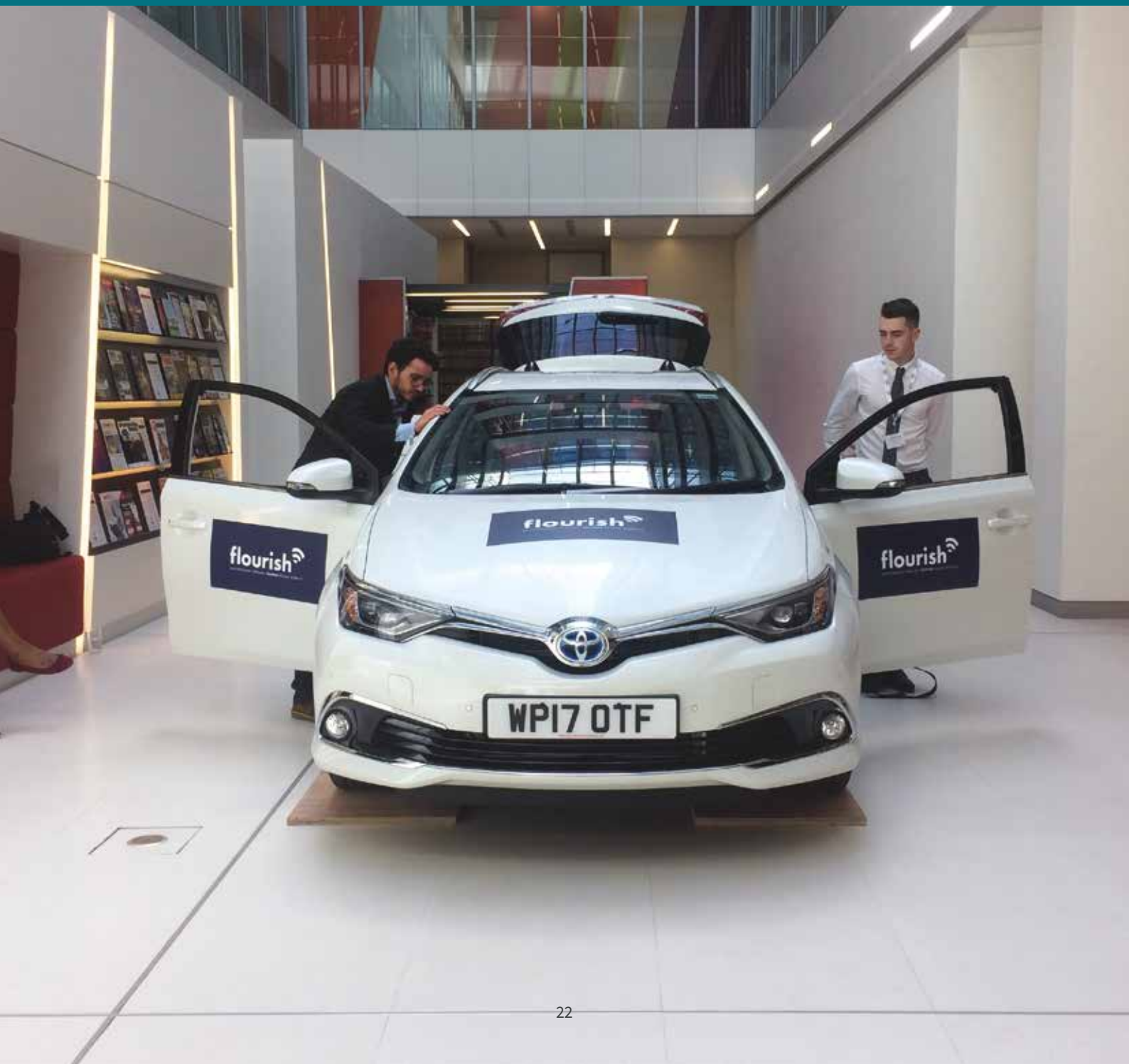
[56] Brian Krzanich, "Data is the new oil in the future of automated driving, https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/)

CHAPTER FOUR: Conclusion

This report explores some of the practical implications of data sharing and cyber-security with a particular focus on user acceptance.

We recognise and welcome the considerable progress that is being made in these areas by government, regulators, industry bodies and stakeholders and are encouraged by the pace of progress and the increasing debate. The data debate is one that will inevitably continue; not least because consumers are, quite rightly, becoming better informed and actively engaged on the potential and positive impact of CAVs on their lives.

Good data governance is not just about regulatory compliance, it is a tool by which to engage and retain customers. For this reason, data and cyber security considerations remain a fundamental component of the success of the CAV ecosystem. Burges Salmon and AXA, together with the FLOURISH consortium, are 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.



Recommendations

Data

The types of data being collected and the uses of that data need to be clear and transparent. Government and industry stakeholders should collaborate to begin to structure a 'data map' for the CAV ecosystem which seeks to identify who needs access to data, what data and when.

A working group made up of the ICO and industry stakeholders should be convened to examine the output of the data mapping exercise and to begin to discuss the frameworks for effective governance of personal data in the CAV ecosystem. This working group should explore the standard data exchanges which will be required for the successful functioning of CAVs together with the appropriate lawful bases.

The ICO should produce guidance on the use of personal data in the CAV ecosystem specifically addressing its views on the ODI's report that journey data constitutes personal data.

A consultation on the changes to current data protection laws should be launched to examine what changes would be necessary in order to facilitate the successful deployment of CAVs on UK roads.

BSI, the UK's National Standards Body should work to develop a data standard to support the UK as a global leader in the CAV technology and the successful deployment of CAV technology.

Cyber Security

The government should continue to invest in cyber security, in particular in relation to cyber security in CAVs. This work should build on the progress made in the last 12 months including through the publication of the Key Principles of Vehicle and Cyber Security for Connected and Autonomous Vehicles.

Investment

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.

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 64 countries, with 103 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, Technical Director AXA Insurance, david.j.williams@axa-insurance.co.uk
Sophie Bonnel, Senior Public Affairs Executive, sophie.bonnel@axa-uk.co.uk

M4(E)
London
Bristol(C)
(M32)
M4(W)
S. WALES
Chepstow
(M48)
A38
Filton
The SOUTH WEST
Bristol(W)
M5
M5

Burges Salmon

Insurance & Legal Report

2018

AXA Insurance UK plc Registered in England and Wales No 78950. Registered Office: 5 Old Broad Street, London EC2N 1AD. A member of the AXA Group of companies. AXA Insurance UK plc is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Telephone calls may be monitored and recorded.