The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles

CHANNON, Matthew and MARSON, James <http://orcid.org/0000-0001-9705-9671>

The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles

Connected and autonomous vehicle (CAV) use, having been tested in various cities around the world and adopted in many areas through public transport, is being prepared for private sector use. The connected dimension of CAV provides for the vehicle to communicate with other vehicles and local infrastructure to operate in a safe manner. Yet, it is this communication of data and operation through software which causes potential problems in the event of the software suffering from unlawful modification (hacking). The consequences of a CAV being hacked could result in its features being compromised resulting in accidents, damage, financial loss, deaths and personal injury. It is also likely that hacking will affect fleets of vehicles operating on the same software version rather than individual vehicles. In this paper we argue there is a need for a strategy to determine how responsibility for the damage and loss caused following the mass hacking of CAVs is to be apportioned. This discussion is presently missing in the evolving literature on CAV maturity and we conclude that a national compensatory body offering a guarantee fund from which victims may seek redress would provide the most appropriate solution for all stakeholders.

Keywords: Connected and autonomous vehicles; insurance regime; mass hacking; motor insurers' bureau; national compensatory body.

1. Introduction

Cybersecurity for CAVs is not a novel topic either in the legal sphere or from an engineering standpoint. Discussion has taken place internationally concerning how to make a vehicle more secure and the role of manufacturers in this process.[1] Liability for CAVs more generally is also certainly not a new topic,[2] however, there has been limited examination of liability for cybersecurity breaches of CAVs.[3] Some discussion has taken place in the US already on who is liable in the US if a CAV is hacked.[4] While this may be useful to examine, its application to the UK is limited due to differing regulation of CAVs, with the UK having introduced the Automated and Electric Vehicles Act (AEVA) 2018.

[1] Charlotte Ducuing, 'Towards an Obligation to Secure Connected and Automated Vehicles "By Design"?' in Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (eds) 'Security and Law Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security' (2019 Intersentia).

[2] There are dozens of articles which address liability of CAVs. For example, Walker-Smith provides a long list of articles in the US in his article. See Bryant Walker-Smith, 'Automated Driving and Product Liability' (2017) 1 Michigan State Law Review. Also see Kenneth S. Abraham & Robert L. Rabin, 'Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era' (2019) 105 Virginia Law Review 127.

[3] See for example, written evidence submitted to the Public Bill Committee House of Commons by Matthew Channon, Aysegul Bugra, Kyriaki Noussia and Professor Rob Merkin QC on the Automated and Electric Vehicles Bill (AEVB 10) October 2017, the written evidence stated at paragraph 11, 'There are a number of potential solutions to the mass-risk issues with regards to hacking, involving separate policies or funds which could compensate in these scenarios'. Also the 'Law and Autonomous Vehicles' book (Chapter 5) contained a brief discussion on who is and should be liable for CAV hacking, the book also briefly noted the potential extension of reinsurance funds although as noted in the book this was an area that needed further research. This article aims to undertake such research. See Matthew Channon, Lucy McCormick and Kyriaki Noussia, The Law and Autonomous Vehicles (2019, Informa) Chapter 5. Also see work by Joshua Prior who examined liability for cyber security breaches, the paper recommended a new central fund for mass-hacking although noted that more research was needed. However, our paper considers the context of the UK and EU's motor insurance regimes in further detail and recommends solutions based on expansion of current regimes. Our paper further considers reinsurance pools in detail as a potential solution. See Joshua Prior, 'Connected and Autonomous Vehicles, Cyber Threats and the UK Motor Insurance Framework. Is the Automated and Electric Vehicles Act 2018 Fit for Purpose?' (2021) 46 Exeter Law Review 126.

[4] Zev Winkelman, Maya Buenaventura, James M. Anderson, Nahom M. Beyene, Pavan Katkar, Gregory Cyril Baumann, 'When Autonomous Vehicles are Hacked, Who is Liable?' (2019) Rand Corporation. Available at https://www.rand.org/pubs/research_reports/RR2654.html.

We begin our study by examining the challenges associated with the hacking of CAVs, on both practical and legal bases, before exploring the regulatory regime and the current issues regarding apportioning responsibility for the consequences of injury and loss associated with a hacked vehicle. We finally present two recommendations for reform to the insurance system of CAVs to ensure that victims are provided with necessary compensation.

2. Challenges with the hacking of CAVs

It is recognised that computers are capable of being hacked with potential for privacy breaches and data loss. CAVs establish attractive targets to hackers due to the information which can be accessed and, for example, sold to third parties or otherwise accessed and thereby used for other criminal activities (for example trafficking drugs or inflicting harm).[5] The introduction of Artificial Intelligence (AI) into society has exacerbated the potential, well documented, risks of hacking.[6] While the extent of any vulnerabilities is not yet clear, due to the technology still developing;[7] CAVs, compared to many other forms of AI, have the added risk of causing both physical injury and property damage.[8] Whereas vehicles with no connectivity require physical access to a vehicle, the connected nature of CAVs adds greater risk, with hacking potentially taking place over wireless networks[9] and therefore with CAVs potentially 'more easily compromised and weaponised to infect other vehicles'.[10] Hacking therefore can cause substantial damage and 'represents a significant caveat to the projections that the proliferation of autonomous vehicles will significantly reduce the frequency of accidents'.[11] The potential for major damage[12] resulting from cybersecurity breaches are of international concern, with jurisdictions such as the UK, the EU, Australia, and the US looking at ways to ensure that CAVs can be secure.

The EU introduced Regulation 2019/2144 which provided for some measures to secure against cyber-attacks.[13] The United Nations Economic and Social Council has also examined this area with the

[5] Chasel Lee, 'Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars' (2017) 69 Federal Communications Law 25.

[6] Of course, CAVs are not the only AI which is prone to hacking which could cause property damage and personal injury. For example, drones could also be hacked and could also cause significant damage. Also see in relation to cyber risk for autonomous ships, Feng Wang, 'The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships' (2020) 4 Journal of Business Law 311. For Cyber Risk and Drones see, Julie-Anne Tarr, Maurice Thompson and Anthony Tarr, 'Regulation, Risk and Insurance of Drones: An Urgent Global Accountability Imperative' (2019) 8 Journal of Business Law 559.

[7] Simon Parkinson, Paul Ward, Kyle Wilson, and Jonathan Miller, 'Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenge' (2017) 18 (11) IEEE Transactions on Intelligent Transportation Systems 2898.

[8] See Parkinson (n 7).

[9] Lee (n 5).

[10] Caleb Kennedy, 'New Threats to Vehicle Safety: How Cyber Security Policy will Shape the Future of Autonomous Vehicles' (2017) 23(2) Michigan Telecom and Technology Law Review 343.

[11] Donald G Gifford, 'Technological Triggers to Tort Revolutions: Steam Locomotives, Autonomous Vehicles, and Accident Compensation' (2018) 11 (1) Journal of Tort Law 132.

[12] Research presented by Derrick Dominic, Sumeet Chhawri, Ryan. M. Eustice, Di Ma, and Andre Weimerskirch, 'Risk Assessment for Cooperative Automated Driving' CPS-SPC'16, October 28 2016, Vienna, Austria. DOI: http://dx.doi.org/10.1145/2994487.2994499 has demonstrated the serious accidents that can result from a hacked vehicle.

[13] See for example Article 4 (5) (d) Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166).

Working Party on Automated Vehicles introducing cybersecurity proposals.[14] So far no legislation has been introduced in the UK which regulates the hacking of CAVs. Moreover, the Law Commission has determined that hacking is outside of its terms of reference for its consultation on AVs, despite noting that cybersecurity was an area of 'major concern'.[15] However, work has been undertaken by the Department for Transport in order to provide guidance on cybersecurity to manufacturers through the Key Principles of Cyber Security for Autonomous Vehicles.[16] Guidance includes ensuring security throughout the lifetime of the product, particularly concerning vehicles of different ages which will be on the road at the same time. The guidance also explains the need to ensure that the technology is resilient in light of any cyber-attack. Of course, due to the international nature of the challenge, recommendations have been made at an international level. For example, the United Nations introduced recommendations concerning over-the-air software updates.[17]

3. Responsibility of insurers to compensate for accidents involving motor vehicles

The liability regime applicable to conventional motor vehicles is well established. In the UK, the Road Traffic Act (RTA) 1988 is the legislative instrument which places obligations on owners of vehicles to maintain, as a minimum, third-party insurance for vehicles used in a public place (subject to, whilst it applies, the *Vnuk*[18] and *Lewis*[19] extension to private land too).[20] This statutory measure is complemented through extra-statutory sources in the event that an innocent third-party victim suffers loss due to the actions of an uninsured or untraced driver. These agreements, the Uninsured Drivers' Agreement (UDA)[21] and the Untraced Drivers' Agreement (UtDA)[22] are established between the Secretary of State for Transport and the Motor Insurers' Bureau (MIB) and had been governed by the EU through a series of expansive directives.[23] The MIB, a private company limited by guarantee,

[14] Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system: Submitted by the Working Party on Automated/autonomous and Connected Vehicles' (23rd June 2020) <http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf>. Note that UN Regulations are binding in the EU.

[15] UK and Scottish Law Commissions 'A Joint Preliminary Consultation Paper on Automated Vehicles' (2018) Law Commission Consultation Paper 240 [1-21].

[16] While we discuss the key principles here in limited depth, you can find more detailed analysis in Channon (n 3).

[17] UN Task Force on Cyber Security and Over-the-Air Issues, Draft Recommendation, UNECE WP.29 GRVA, 20 September 2018, at <https://www.unece.org/fileadmin/DAM/trans/doc/2018/wp29grva/GRVA-01-17.pdf>.

[18] Case C-162/13 *Damijan Vnuk v Zavarovalnica Triglav* [2014] EUECJ C-162/13. [2016] RTR 10.

[19] *MIB v Lewis* [2019] EWCA Civ 909.

[20] Section 143 of the RTA 1988. For commentary on the evolution of the case law here see James Marson and Katy Ferris, 'For the Want of Certainty: Vnuk, Juliana and Andrade and the Obligation to Insure' (2019) 82(6) Modern Law Review 1132; James Marson and Katy Ferris, 'The Compatibility of English Law with the Motor Vehicle Insurance Directives: The Courts Giveth…but will Brexit Taketh Away?' (2020) 136 Law Quarterly Review 35; and James Marson and Katy Ferris, 'Too Little, Too Late? Brexit Day, Transitional Periods and the Implications of MIB v Lewis' (2020) 3 European Law Review 415.

[21] In the event of accident being caused, or contributed to by, a driver who was uninsured at the time (holding no valid policy of insurance), but who, by the nature of the event is identified, the MIB will consider dealing with the claim for compensation from the victim.

[22] This applies to victims of an accident where the driver deemed responsible for the accident leaves the scene without identifying him/herself and cannot be traced. The MIB will consider claims of compensation in respect of damages to property and personal injury.

[23] (The First Directive) Council Directive 72/166/EEC on the approximation of the laws of Member States relating to insurance against civil liability in respect of the use of motor vehicles, and to the enforcement of the obligation to insure against such liability [1972] OJ L103/1; (The) Second Council Directive 84/5/EEC on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles [1984] OJ LL8/17; (The) Third Council Directive 90/232/EEC on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles [1990] OJ L129/33; Directive 2000/26/EC on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles and amending Council Directives 73/239/EEC and 88/357/EEC (The Fourth Motor Insurance Directive) [2000] OJ L181/65; (The Fifth Directive)

operates to reduce the negative consequences for victims of road traffic accidents caused by uninsured or untraced drivers in the UK (and of foreign drivers through the 'green card scheme').[24] To provide this function to the national motor vehicle insurance scheme it acts as an insurer of last resort for victims who would otherwise be left without a remedy to access compensatory redress.[25] The MIB funds this guarantee reserve through a levy imposed on the insurance companies who operate in the UK, each of whom must be a member of the Bureau.[26]

Further, and before examining potential responsibility being applied to insurers to compensate for vehicle hacking, it is important to put into context the insurance regime for purposeful damage caused by conventional vehicles, due to the similarity of the objectives of both conventional and automated vehicle regimes, to protect third-parties. Moreover, the relevant statutory wording is similar in both the AEVA 2018 and RTA 1988. For example, both the conventional vehicle and CAV statutes use the word 'accident' which is, prima facie, a challenge for the applicability of laws to purposeful damage. Importantly, the RTA 1988 provides that the user must insure against 'accidents caused by or arising out of their use of the vehicle'.[27] The overriding objective of protecting third-party victims means that where the insured commits damage purposefully, the injured victim must still be compensated. As noted by the Court of Appeal in *Hardy v Motor Insurers' Bureau*:

> The policy of insurance which a motorist is required by statute to take out must cover any liability which may be incurred by him arising out of the use of the vehicle by him. It must, I think, be wide enough to cover, in general terms, any use by him of the vehicle, be it an innocent use or a criminal use, or be it a murderous use or a playful use.[28]

The protective policy of conventional motor insurance is seen in the Court of Appeal judgment, albeit *obiter*, in *Charlton v Fisher*[29] determined that the policy of safeguarding third party protection effectively overrides the ordinary interpretation of the legislation in a third-party context.[30] Moreover, *Bristol Alliance v Williams*[31] provides that where purposeful damage is not covered by the policy, the victim must be compensated, although under the UDA.[32] The application of policy therefore to

---

Directive 2005/14/EC amending Council Directives 72/166/EEC, 84/5/EEC, 88/357/EEC and 90/232/EEC and Directive 2000/26/EC of the European Parliament and of the Council relating to insurance against civil liability in respect of the use of motor vehicles [2005] OJ L149/14; and (The Sixth Directive) Directive 2009/103/EC relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability [2009] OJ L263/11.

[24] The 'green card scheme' applies to accidents caused through the negligent driving of foreign motorists. Here the MIB may deal with the victim's claim for damages to property or personal injury rather than require them to seek communication from the foreign insurer.

[25] Memorandum and Articles of Association (1946, as amended by special resolution passed on 7 June 2012) Motor Insurers' Bureau; see http://www.mib.org.uk/NR/rdonlyres/32A4AB2C-5B4A-43A8-8610-1A629B7A933B/830/ArticlesofAssociation070612.pdf, pp.2-4.

[26] See ss. 95, 143 and 145(2) of the RTA 1988.

[27] Section 145 of the RTA 1988.

[28] *Hardy v Motor Insurers' Bureau* [1964] 2 QB 745, 760.

[29] [2001] 3 WLR 1435.

[30] Note the author discussed the term 'accident' and *Charlton v Fisher* in Matthew Channon (n 3), noting that the courts should interpret the term purposely for the AEVA 2018 to include deliberately caused damage.

[31] [2012] EWCA Civ 1267.

[32] Motor Insurers' Bureau 'Uninsured Drivers' Agreement' (2015). <https://www.mib.org.uk/media/166917/2015-uninsured-drivers-agreement-england-scotland-wales.pdf>. It is important to note that under Article 75 of the MIB's articles of association the insurer is required to compensate as an agent of the MIB, although compensation is paid under the MIB Agreement rather than the insurance policy. It is notable that the MIB Uninsured Drivers' Agreement had previously excluded compensation for Acts of Terrorism in Article 9 although this was later removed by the MIB in its Uninsured Drivers Supplementary Agreement. Motor Insurers Bureau 'Articles of Association' <https://www.mib.org.uk/media/462763/2019-mib-articles-of-association-030719.pdf>. See Motor Insurers' Bureau, 'Supplementary Uninsured Drivers' Agreement 2017' <https://www.mib.org.uk/media/350345/2017-supplementary-uninsured-drivers-agreement-england-scotland-and-wales.pdf>.

purposeful damage from conventional vehicles is a potential direction for CAVs. As we will see in part 5, the AEVA 2018 has been drafted with such protective purpose, and this could signal an approach which establishes the insurers' cover for purposeful damage from CAV use. The next section examines product liability and whether this could provide an answer.

4. Product Liability

The previous section outlined the applicability of the insurance market in providing protection to road users in the event of accidents, including the mass hacking of CAVs and resultant damage. Thus, during the implementation phases of CAV use and its development along the SAE scale[33] towards full self-driving modes, and until the point where persons behind the wheel are considered passengers rather than drivers,[34] the current system of compulsory motor vehicle insurance will continue. This includes provision for the recovery of damages for both accidental and intentional damage by the innocent third-party. We now consider whether and to what extent the vehicle manufacturer may be subject to responsibility for defects in software (which will fundamentally operate the CAV) where these have been modified by an unauthorised external actor (rather than through bugs and errors during 'normal' software update roll-outs). This is most likely achievable through recourse to protections available through product liability law.

4.1 Product liability as applied to software

Under s. 5 of the AEVA 2018 (we discuss the AEVA 2018 in more detail in part 5) insurers have a right of recourse against the person responsible for the motor accident. This is likely to be the manufacturer of the vehicle in product liability[35] under the Consumer Protection Act 1987 (CPA 1987), although claims could involve the fleet operator of the vehicle in negligence.[36] Product liability, compared to negligence, does not require proof of fault, but rather proof that the product is defective (s. 2 CPA 1987, as discussed in respect of the interpretation of defectiveness, below) although notably only applies to products, a potentially significant challenge in terms of claims from hacked vehicles. If not, the insurer would be unable to claim against the manufacturer under product liability for cybersecurity breaches due to software defects, and instead would need to pursue a claim in negligence as the manufacturer is deemed to owe a duty of care to the end consumer.[37] The

[33] The Society of Automotive Engineers (SAE) International Standard J3016 which identifies the levels of automation of vehicles. At level 0, the driver controls all aspects of driving. Level 1 includes steering and acceleration/deceleration assistance systems aiding the driver. At level 2, partial automation provides steering and acceleration/deceleration using information from the driving environment. The driver is expected to intervene and respond when requested at Level 3, but all other aspects of driving is taken by the CAV. Level 4 denotes high automation where the automated system takes all aspects of driving. Level 5 is used to describe an automated driving system where all tasks in all roadway and environmental conditions are taken by the system. This refers to a full automation system.

[34] James Marson and Katy Ferris, 'The Lexicon of Self-Driving Vehicles and the Fuliginous Obscurity of 'Autonomous' Vehicles' (2021) Statute Law Review https://doi.org/10.1093/slr/hmab016.

[35] Note that the CPA 1987 extends not just to the 'producer of the product' (s. 2(2)(a) of the CPA 1987) but also under s. 2(2)(b) 'any person who, by putting his name on the product or using a trade mark or other distinguishing mark in relation to the product, has held himself out to be the producer of the product; (c) any person who has imported the product into a member State from a place outside the member States in order, in the course of any business of his, to supply it to another'. For discussion see Channon, McCormick and Noussia (n 3).

[36] See Ducuing (n 1) [6.1] who noted the importance of the fleet operator and particularly their role in testing of CAVs who may be required to intervene.

[37] See *Donoghue v Stevenson* [1932] AC 562. However, a negligence claim may be difficult due to the requirement of fault, i.e. that the manufacturer acted below the standard of care required of them, so they acted as a reasonable manufacturer would have done in that same situation. The difficulty, therefore, in terms of cyber security is that the manufacturer may have acted appropriately in the circumstances and could not have avoided a hacking incident. Negligence may prove a popular route to take particularly in economic loss cases which are not covered under product liability.

definition of product has been addressed significantly in literature[38] but requires clarity. The UK Law Commission has been consulting on whether the definition of software should be clarified, noting that this issue should be reviewed, albeit 'not simply for AVs'.[39] Currently any software provided in physical form such as a disk would likely be deemed a product, whereas software over the air is a debatable entity.[40] Moreover, if software is produced by the manufacturer and not a separate component manufacturer, it is likely to be a product. The likelihood, however, is that the software and hardware would be produced by different component manufacturers. Deeming software a product (with the AEVA 2018 applied rather than a more difficult negligence claim) would likely mean significant additional claims and financial burdens against component manufacturers (particularly those who produce software, and could therefore pose a chilling effect on innovation).[41] Much depends on whether the vehicle manufacturer has a contract with the original equipment manufacturer (OEM) to recover compensation paid under the Act. There are also further complicated scenarios around who would be deemed the 'producer' of a product, with potential attribution to individual distributors and individual physical and software component manufacturers.[42] A discussion determining the issue of product liability as applied to software is not the central aim of this paper, but it is arguable that where software is an essential component of a product, and updates are installed by a manufacturer (such as with Tesla) or at mandatory car service/maintenance intervals, the software could be considered a tangible product and be covered by product liability.

4.2 Product liability: Safety and security

If software is a product, the claimant would need to prove that the software was defective, with the product not meeting the consumer's expectation of safety. As noted by Schellekens, '"safety" is not the same as security, but in this context, the two are not unrelated either. A security vulnerability has the potential to become a safety issue. For example, security vulnerability may mean that a hacker can enter the systems of a car'.[43] This is an important point. Yet, as we noted above, the determination of safety is difficult and further difficulties exist in terms of defectiveness. In some circumstances, defectiveness may be easy to spot, as noted by Rand, 'Although locating the vulnerability in the AV system may require significant expertise and expenditure, it will likely be possible—at least in some instances—to locate specific flaws in specific components or software'.[44] However, in many other circumstances defectiveness may be harder to evidence. As noted in a European Parliament report, 'Product defects would be very difficult to prove. Moreover, it would be even more difficult to attribute liability if all necessary software was installed but cybercrime nevertheless occurred'.[45] The

[38] The discussion around product liability and software is not a new one. See for example, Diane Rowland, 'Liability for Defective Software' (1991) 22 Cambrian Law Review 78. Also, the rationale behind not treating software as a product was explored in Maurice Jamieson, 'Liability for Defective Software' (2001) May Journal of the Law Society of Scotland. More recent discussion can be found in Matthew Channon et al (n 3); and Matthew Channon, 'Automated and Electric Vehicles Act: An Evaluation in Light of Proactive Law and Regulatory Disconnect' (2019) 10(2) European Journal of Law and Technology. Also see Joshua Prior (n 3) 151.

[39] See UK and Scottish Law Commissions 'Automated Vehicles: Summary of Responses to Consultation Paper 3 and Next Steps' (2021) https://s3-eu-west-2.amazonaws.com/lawcom-prod-storage-11jsxou24uy7q/uploads/2021/07/Summary-of-the-responses-to-CP3-and-next-steps-1.pdf 24

[40] See for example Stephen Saxby, 'Encyclopaedia of Information Technology Law' (Sweet and Maxwell) 7.132.

[41] Maurice Schellekens, 'No-fault Compensation Schemes for Self-driving Vehicles' (2018) 10(2) Law, Innovation and Technology. 314. DOI: 10.1080/17579961.2018.1527477.

[42] See Saxby (n 41) which highlights potential scenarios concerning producers.

[43] Maurice Schellekens, 'Car Hacking: Navigating the Regulatory Landscape' (2016) 32 Computer Law and Security Review 307, 313.

[44] Winkelman et al. (n 4).

[45] See European Parliamentary Research Service, 'A Common EU Approach to Liability Rules and Insurance for Connected and Autonomous Vehicles: European Added Value Assessment' (2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf> 26.

requirement of defectiveness in the CPA 1987, while stringent, is not one of perfection.[46] Nor just because a vehicle was hacked, and caused damage does it necessarily mean that the vehicle is defective. The authors in Clerk and Lindsell importantly note that, 'merely because some cars have special safety features such as anti-lock brakes, this does not necessarily mean that cheaper models without such features are therefore defective'.[47] Likewise the absence of security features of more advanced models may not necessarily result in a 'defective product'. The reasonable expectations test is therefore cost-benefit with 'safety… traded off against cost and convenience'.[48] The courts will examine several factors with each case being determined on its own facts.[49] This can include, for example, whether the vehicle has regulatory approval, the benefits of introducing the vehicle and the cost of remedying any defect. As was noted previously, the first of these is an important factor and could have a significant link to the AEVA 2018, as if a vehicle is listed as an 'automated vehicle' under the AEVA 2018 (s. 1(1)), a product liability claim is likely to be more challenging.[50] It is evident, therefore, that the definition of 'safety' within the AEVA 2018 will be significant when determining a cybersecurity claim. However, this, of course, is not the only factor to be taken into account. The difficulty is that the 'courts must simply weigh competing factors intuitively'.[51] Moreover, the disparity in case law concerning 'defective product' means that 'producers have little guidance on when they can expect their products to be deemed defective'.[52] These are important points and with significant applicability challenges for new technologies. Further, while the outcome of a case is likely to be fact specific due to the multi factorial approach, the absence of case law concerning how such an approach would be applied in a CAV context adds to the difficulty. The absence of legislative clarity in the AEVA 2018 and what is deemed to be safe in a cybersecurity context also adds to the struggle.

Such confusion could therefore mean difficulty in resolving the outcome of disputes between insurer and manufacturer. Disputes were envisaged by the legislature, hence the requirement that third parties are compensated under strict liability. Moreover, manufacturers may attempt to use defences against insurers. For example, manufacturers may argue that the ten-year time limit on claims from the introduction of the product had ended. The ten-year defence could be complicated for software and it is uncertain as to whether a CAV would be deemed a new product once updates have been provided. If so, new software updates could restrict the defence significantly for the overall vehicle.[53] Nevertheless, even with such defence restricted and the likelihood of vehicles lasting significantly longer than ten years, the defence could cause a 'liability vacuum'.[54] Probably the most complicated

---

Also see Ryan J Duplechin, 'The Emerging Intersection of Product Liability, Cyber Security and Autonomous Vehicles' (2017) 805 Tennessee Law Review 803 which noted that defects 'may become apparent but unrecognisable'.

[46] As was noted in by Michael Jones, Anthony Dugdale and Mark Simpson, Clerk and Lindsell on Torts (2017 Sweet and Maxwell 22nd edition). Also see Donal Nolan, 'Strict Products Liability for Design Defects' [2018] 134 (Apr) Law Quarterly Review 176.

[47] Jones et. al. (n 47).

[48] As noted by Donal Nolan (n 47), 178.

[49] See Robert Veal and Henrik Ringbom, 'Unmanned Ships and the International Regulatory Framework' (2017) 23(2) Journal of International Maritime Law 100, 113. The authors in this article discuss product liability for Unmanned Ships and note the lack of case law in terms of product liability and defect. There are some similarities here with CAVs. For example, the authors note in terms of unmanned ships that, 'The range of different types of technical issues is broad. The division of liability between the shipowner and, for instance, the shipbuilder or the manufacturer of an individual component is not always easy to draw'. The division of liability here is comparable to questions around the division of liability between the CAV owner and the manufacturer, with technical issues undoubtedly broad and the division of liability between the vehicle owner or manufacturer not always easy to draw.

[50] *Wilkes v De Puy International Ltd* [2016] EWHC 3096.

[51] Jacob Eisler, 'One Step Forward and Two Steps Back in Product Liability: The Search for Clarity in the Identification of Defects' (2017) 76(2) Cambridge Law Journal 230, 235.

[52] Eisler (n 52).

[53] See Jan De Bruyne and Jarich Werbrouck, 'Merging Self-driving Cars with the Law' (2018) 34 (5) Computer and Security Law Review 1150, 1153.

[54] De Bruyne and Werbrouck (n 54).

defence concerning software is the state-of-the-art defence.[55] That the state-of-the-art at the time was not such that the fault could be discovered. This particular defence and its application to CAVs and software has been a point of unease for manufacturers, with the Society of Motor Manufacturers noting, 'While vehicle manufacturers have to meet state-of-the-art criteria for the whole vehicle when introducing it to the market, software developments are constantly and fast evolving. What is deemed state-of-the-art for software today may no longer be state-of-the art tomorrow'.[56] Determining software's state-of-the-art poses a challenge for both courts and manufacturers, the shifting cybersecurity risk provides that manufacturers will need to be constantly aware of changes in risk and security. Evidently while manufacturers are in favour of the state-of-the-art defence, there is an alternative view as to whether the defence should be maintained for new technologies. As noted by the Report from the EU Expert Group on Liability and New Technologies, 'the producer should be strictly liable for defects in emerging digital technologies even if said defects appear after the product was put into circulation, as long as the producer was still in control of updates to, or upgrades on, the technology. A development risk defence should not apply'.[57] The control of software through updates allows the manufacturer to remedy defects when known. Of course, it would be difficult to provide such a defence where software could be made more secure by the manufacturer with the potential of disincentivising the manufacturer in producing updates. However, such a defence is particularly relevant in terms of fast-moving cybersecurity standards.

4.3 Product liability and the problem for third-party victims

A user in these circumstances would not, typically, find themselves liable in negligence for the consequences of resultant damage. However, it is clear that product liability protects users of the product and it is uncommon for third-party losses to be experienced in the use of products mainly of a consumer variety. CAVs will be used for personal and commercial purposes, they will have much greater access to the public and users beyond the typical consumer products envisaged under the existing statutory scheme. If the system to be adopted for the consequences of digital problems with the vehicle was left to the individual driver to be responsible, tortious liability would be ineffective due to the general problem of a lack of resources to satisfy such claims. This would, potentially, expose victims to an inability to secure compensation and thus their access to justice would be compromised. Further, without a recognised compensatory scheme in place, public trust in the use of CAVs could be placed in jeopardy. The system would therefore need replacing through insurance cover which would enable the protection of third-party victims. However, a concern exists with a model of insurance which involves the consequences of hacking. As has been demonstrated, the consequences of hacking of a CAV can be to affect the fundamental safety and functionality of a motor vehicle. This, save for the driver disregarding software critical updates or disabling/modifying the software operating the vehicle, would have nothing to do with the driver and it would be unlikely that such a driver would even be able to ascertain if a software compromising situation had taken place. It is also problematic given that, unlike a mechanical failure, hacking may involve a third-party taking active control over the vehicle. Thus, in this example, the vehicle is being manipulated beyond the control of the driver and/or any other person within the vehicle for which the driver would, under the RTA 1988, be held responsible. This creates a lacuna in the compensatory protection of all involved in the use of CAVs. Hacking also, of course, raises other issues which are beyond the scope of this paper to adequately discuss. By its nature, hacking can lead to an unauthorised third-party taking control of the software operating the vehicle hardware, leading to an accident-causing loss. It can also, as noted earlier, lead to data breaches and the theft of information and data held in the

[55] Also known as the Development Risk Defence.
[56] Society of Motor Manufacturers and Traders, 'Connected and Autonomous Vehicles: Position Paper' (February 2017) <https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf>.
[57] Report from the Expert Group on Liability and New Technologies, 'Liability for Artificial Intelligence and Other Emerging Digital Technology' (European Commission 2019) [14]. Also see Francesco Paolo Patti, 'The European Road to Autonomous Vehicles' (2019) 43 (1) Fordham International Law Journal 125 who was also in favour of abolishing the development risk defence.

vehicle and its communications with external infrastructure which could ultimately result in fundamental rights violations.[58]

4.4 Apportioning responsibility between insurers and manufacturer

The above, therefore, highlights potential disputes between the manufacturer and insurer. However, disputes are likely to be costly and therefore, manufacturers and insurers are likely to have commercial agreements to determine liability.[59] This is unlikely to remove the need for the investigation of defects, as manufacturers will have agreements with OEM's to recover compensation, dependent on the parts which have caused the damage. Manufacturers may also obtain additional insurance to cover themselves for any reclaim by insurers, meaning potential disputes between insurers. Cybersecurity breaches may cause further difficulties due to the potential costs damage, particularly for mass hacking incidents. Whether the agreement between the manufacturer and insurer would cover for this is uncertain. It seems that insurers are against coverage for mass hacking, even where such cost could potentially be recovered from the manufacturer.[60] This is likely due to the potential costs involved if a fleet of vehicles were hacked and caused significant physical damage. Nevertheless, there are undoubtedly considerations concerning claims by insurers and defence of claims by manufacturers, such as an insurer's refusal to provide cover.[61] This is pertinent in a cybersecurity context with substantial mass hacking costs, with insurers potentially unwilling to take this on.[62] However, if manufacturers are required to pick up the burden of compensating victims of mass-hacking, major disruptions to innovation would be likely.[63] Furthermore, for both manufacturer and insurer, disputes could result in litigation costs.[64] Of course, it is difficult to envisage whether either the manufacturer or insurer of the CAV would be willing to accept the cost of large scale claims or this may lead to very complex disputes.

The above sections have attempted to briefly explore the problems present in the tortious and insurance sectors as they apply to CAV introduction on roads in the UK. Indeed, it might be argued that at this stage it is unclear where responsibility for compensation for hacking or mass hacking of CAVs would arise.[65] Given these concerns, we continue by assessing the effectiveness of the legislative instrument developed to facilitate the introduction of CAVs through its regulation of insurance and the protections available for CAV users and third-parties.

5. The AEVA 2018

The AEVA 2018[66] provides a route to compensation for the victim against an insurer where a CAV causes an accident whilst 'driving itself'. Proof of fault is not required, nor is proof of defectiveness.[67]

[58] See, for example, James Marson, Matthew White and Katy Ferris 'The Investigatory Powers Act 2016 and Connected Vehicles: A New Form of Panspectric Veillance Looming' (2022) forthcoming.
[59] As was noted in the Department for Transport (DfT) 'Pathway to Driverless Cars: Consultation on Proposals to Support Advanced Driver Assistance Systems and Automated Vehicles Government Response' (2017) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581577/pathway-to-driverless-cars-consultation-response.pdf> [3-14].
[60] ibid, 18,
[61] ibid [3-14].
[62] See previous scepticism from insurers concerning mass hacking risks.
[63] See Channon (n 39) which cites Maurice Schellekens (n 44) on the 'chilling effect' of liability law on manufacturers.
[64] As we noted above, there is potential significant expenditure in finding defects.
[65] See Channon (n 39).
[66] For further analysis of the Automated and Electric Vehicles Act 2018 see Channon et al (n 3); Felix Boon, 'Two Bites of a Peculiar Cherry? Res judicata, Time Bar and Illiquid Debts: Insurer Recoveries under the Automated and Electric Vehicles Act 2018' (2020) British Insurance Law Association Journal; and James Marson, Katy Ferris and Jill Dickinson, 'The Automated and Electric Vehicles Act 2018 Part 1 and Beyond: A Critical Review' (2019) Statute Law Review, hmz021, https://doi.org/10.1093/slr/hmz021.

Once the victim is compensated, the insurer is able to recover from the responsible party. It can be assumed that the basis of this aspect of the AVEA 2018, was likely to be a claim against the manufacturer under the laws of product liability (the CPA 1987) for defects relating to software updates which lead to the accident. Importantly, the AEVA 2018 only applies to an 'automated vehicle', a vehicle which is 'capable of driving itself safely' (s. 1(1) AEVA 2018), and the challenges surrounding the definition of an automated vehicle, particularly concerning 'safely', have been discussed in the literature.[68] However, further challenges exist including the extent that a CAV must be cybersecure for it to be deemed 'safe'. While there are approaches to determine whether measures have taken place to ensure cybersecurity,[69] any potential software vulnerabilities will often only be found when a vehicle is hacked. Consequently, vehicles with significant cyber vulnerability could originally be deemed safe, with vulnerabilities noticed when a cyber-attack has already occurred. Further, it may not always be possible to secure a vehicle against cyber-attacks as vulnerabilities will be present in any system. In fact, even in product liability claims against the manufacturer under the CPA 1987, the insurer does not need to prove absolute safety[70] but rather that the, 'safety of the product is such as persons generally are entitled to expect'.[71] As will be noted, safety in the CPA 1987 and the AEVA 2018 are likely to be linked, with product liability claims, at least in part, based on whether the standards in the legislation have been met.[72]

'Driving itself' is a key term within the AEVA 2018, used both in its definition of 'automated vehicle' and in the core provision which sets out the insurers' requirement to compensate the victim (s. 2(1) AEVA 2018). As noted in s. 8 AEVA 2018, 'a vehicle is "driving itself" if it is operating in a mode in which it is not being controlled, and does not need to be monitored, by an individual.' This, prima facie, excludes vehicles which are being hacked, as vehicles are unlikely to be under the control of the individual / person behind the wheel (and the legislation clearly could not be construed at present to include reference to a hacker in these circumstances).[73] The Centre for Connected and Autonomous Vehicles in its August 2020 Consultation on Automatic Lane Keeping Systems (ALKS) provided a suggestion for the interpretation of control noting that, 'A vehicle is not being 'controlled' by an individual if the individual controls none of the following: 1 Longitudinal dynamics (speed, acceleration, braking, gear selection); 2 Lateral dynamics (steering)'.[74] Interestingly the Consultation's application of this to ALKS stated, 'The activated system (ALKS) shall perform the DDT (Dynamic Driving Task) shall manage all situations including failures, and shall be free of unreasonable risks for the vehicle occupants or any other road users'.[75] This would limit the potential for vehicles with significant cyber vulnerabilities from being included within 'controlled'. Nevertheless, even if prone vehicles were encompassed within this, the future definition of 'safety' may well preclude these vehicles. However, 'unreasonable' clearly connotes that 'reasonable risks' would be acceptable. This is required due to the overall risk, yet the extent that these risks become 'unreasonable' is uncertain. If the Key Principles of Cyber Security and other UN regulations are followed, this may provide an example of a reasonable risk. Of course, while a vehicle with significant known cyber vulnerabilities may not be listed as an automated vehicle under the AEVA 2018, vehicles which later are hacked may be classed as 'driving itself' for the purpose of the Act,

---

[67] If the vehicle is being manually driven then coverage would be provided by the insurer as per insurance for conventional vehicles under the RTA 1988.
[68] See Marson and Ferris (n 35).
[69] Such as whether the manufacturer has followed the Key Principles of Cyber Security as well as the PAS 1885:2018 *'The fundamental principles of automotive cyber security'*.
[70] See Nolan (n 47) who also quotes Hickinbottom J in *Wilkes v De Puy International Ltd* [2016] EWHC 3096 (HC) [65], who provided 'inherently and necessarily a relative concept.'
[71] Section 3 of the CPA 1987.
[72] *Wilkes v De Puy International Ltd* [2016] EWHC 3096 (HC).
[73] See also discussion from Prior (n 3) in terms of internal and external control.
[74] Centre for Connected and Autonomous Vehicles, 'Safe Use of Automated Lane Keeping System (ALKS) Call for Evidence: Moving Britain Ahead' (August 2020) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/911016/safe-use-of-automated-lane-keeping-system-alks-call-for-evidence.pdf> [3.14].
[75] ibid (Annex A).

resulting in contrasting interpretations within the Act. However, there is clear legislative intent that victims of hacked vehicles would be encompassed within the Act. In the consultation pre-AEVA 2018 the government envisaged that hacked CAVs would be covered,[76] a position taken in the House of Commons Public Bill Committee Debates.[77] While neither of these establish binding authority, they could be useful to a court when determining whether hacked vehicles would be encompassed within the Act. Moreover, the policy rationale, to protect third-party victims, provides a strong justification to ensure wide interpretation. The alternative to the AEVA 2018, the need to claim from the manufacturer directly in negligence or product liability, would unlikely fulfil this policy rationale.

Notably, the AEVA 2018 attempts to fulfil the policy rationale of victim protection and seemingly affords greater protection than the regime for conventional vehicles. For example, the AEVA 2018 greatly restricts the contractual freedom between insurers and policyholders, as insurers are unable to utilise policy exclusions[78] against third-parties. The only exception being under s. 4,[79] with insurers able to exclude liability to, or recover compensation from,[80] the 'insured person' in case of a failure to update software which the 'insured person' 'knows or ought to know is safety critical' (s. 4(1)(b) AEVA 2018) or if software is introduced without permission (s. 4(1)(a) AEVA 2018).[81] Updates are deemed 'safety critical' if it would be unsafe to use the vehicle without the software being installed (s. 4(6)(b) AEVA 2018). This is relevant to vehicle hacking due to the cybersecurity risks resulting from outdated or malicious software. The provision is intended to act as a deterrent to prevent 'insured persons' from installing prohibited software, whilst also providing an incentive to update necessary software. Whether this will deter/incentivise is uncertain, although the recovery of compensation from the 'insured person' is dependent on funds. However, putting the onus on the insured person, who may have limited knowledge of the importance of a particular update, is difficult, and could lead to unjust results. Manufacturers will need to provide adequate notice and information to the insured person about the necessity of installing such updates. The absence of a warning is likely to point to vehicle defectiveness.[82] In fact even with a warning, a potential product liability claim could be brought against the manufacturer, diminishing the deterrent effect of this provision. As noted in the Venturer Report: 'In the case of a SAE Level 3 or Level 4 vehicle,[83] there is an identifiable product liability issue in respect of a connected AV which is permitted by design to enter automated driving mode in full knowledge that it is unsafe because it is in default of a safety-critical update'.[84] Moreover, in the Report it was noted that where an accident is caused by a vehicle as a result of it not

[76] See Department for Transport (n 60).
[77] See John Hayes MP, House of Commons Public Bill Committee p140.
[78] Exclusion clauses are limited in third party conventional motor insurance although not prohibited (see section 148(2) of the RTA 1988 for a list of prohibited exclusions). Also as noted above, where a non-prohibited exclusion clause is used, the insurer would still be required to compensate as an agent of the MIB. Compensation would be paid in these circumstances under the MIB UDA 2015 and not the insurance policy.
[79] Section 2(6) Automated and Electric Vehicles Act 2018. Also see the DfT Government Response to Consultation (n 60) [3.13].
[80] For recovering compensation see (s. 4(4)(a) of the AEVA 2018).
[81] Where the insured person is not the policy holder but is permitted to drive the vehicle, s. 4(2) provides the insured cannot exclude liability unless they had known that the updates were prohibited and s. 4(4) provides the same for insurer recovery of damage paid to third parties.
[82] See s. 3(2)(a) of the CPA 1987.
[83] For the sake of clarity, the standards mentioned in this quote refer to the Society of Automotive Engineers (SAE) International Standard J3016 which identifies the levels of automation of vehicles. At level 0, the driver controls all aspects of driving. Level 1 includes steering and acceleration/deceleration assistance systems aiding the driver. At level 2, partial automation provides steering and acceleration/deceleration using information from the driving environment. The driver is expected to intervene and respond when requested at Level 3, but all other aspects of driving is taken by the CAV. Level 4 denotes high automation where the automated system takes all aspects of driving. Level 5 is used to describe an automated driving system where all tasks in all roadway and environmental conditions are taken by the system. This refers to a full automation system.
[84] Venturer Project, 'Driverless Cars: Liability Frameworks and Safety by Design' (Venturer, Insurance and Legal Report 2018) 40. <https://www.venturer-cars.com/wp-content/uploads/2018/06/Year-3-Legal-and-Insurance-Report.pdf>.

having up-to-date software installed, this would likely be a defect in the product.[85] These are both important points. Of course, vehicles should be aware of any faults to safety critical functions according to the Key Principles of Cyber Security and should be resilient and 'fail safe' in light of any safety critical faults.[86] In the US, the SPY Car Act 2017 mandated vehicles to be able to immediately identify, stop and report any attempts made to seize control of the vehicle.[87] The absence of such fail safe, would not meet the reasonable expectations test, as a consumer would likely expect that the system was able to limit or prevent damage. Notably where software is not updated, a claim against the manufacturer is more likely than a claim against the insured person, with the manufacturer likely to have deeper pockets.[88] Of course, much depends on whether the software is deemed a product and any potential defences the manufacturer has.

Overall it is evident that the AEVA 2018 is aimed at providing the victim with damages. Whether the AEVA 2018 covers hacking requires clarification. Vehicle safety is likely to be a very important part of the Act relating to hacking and again needs clarity. In concluding this section, we wish to reiterate our argument that to facilitate the adoption of CAVs on a broad scale, public confidence requires a system of insurance to be available in the event of hacking or mass hacking (which by its nature would likely cause significantly greater damage than individual error, software glitches on individual vehicles and so on). Public confidence will be more likely achieved through users and non-users knowing a system of insurance is available to be called upon in such an event. This currently exists with conventional vehicles where the vehicle which is responsible for an accident is uninsured or unidentified, the third-party victim has a central fund from which to claim compensation (the MIB). It also exists in a similar way to the pooling of property insurance for flood susceptible areas where private insurers will either not provide cover, or the premiums would be prohibitively expensive for individual policyholders. In the next part, we examine the proposition of an alternative insurance system for low cost hacking and the introduction of a Maliciously Compromised Connected Vehicle Agreement.

6. Proposing an alternative insurance system for low-cost hacks

One of the intended benefits of CAVs is the removal of driver-error which leads, or contributes to accidents.[89] It will not prevent accidents from taking place on public roads. Software will malfunction and accidents will still occur. The key difference with regards to hacking is the unintended consequences of this activity. For the driver, warnings of software changes, of malfunctioning systems, of critical problems in the operation of the vehicle will likely be unnoticed. As such, the driver may perhaps be unwilling to use CAVs unless either the insurance industry will take responsibility for such consequences or until another system is in place. Systems of compulsory insurance exist in most jurisdictions and, in the EU for example, was regulated through the Motor Vehicle Insurance Directives (MVID)[90] which sought to harmonise insurance cover, albeit not general civil liability, for incidents involving motor vehicles. The onus from the system of insurance was that the driver/owner of the vehicle (through their insurers) would be liable for accidents caused by their vehicle and would, in many respects, enable a third-party victim to bring their claim directly against the insurer. Thus, victim protection was of paramount concern. This had already been demonstrated

[85] Venturer Project (n 85), 41.
[86] Key Principles for Cyber Security (n 70) Principle 8.2.
[87] SPY Car Act (2017). S. 680, SPY car Act of 2017, 115th United States Congress. https://www.congress.gov/bill/115th-congress/senate-bill/680.
[88] For discussion on the extent of deep pockets theory see Victor E. Schwartz, Phil Goldberg and Christopher E. Appel, Deep Pocket Jurisprudence, 'Where Tort Law Should Draw the Line' (2018) 70 Oklahoma Law Review 359.
[89] For instance, there are over 31 million vehicles on Britain's roads and around 93% of all crashes are attributed to human error. See Ian Kemp, 'Autonomy & Motor Insurance. What Happens Next?' (2018) An RSA report into autonomous vehicles & experiences from the GATEway Project. https://www.rsagroup.com/media/2830/rsa-report-autonomy-and-motor-insurance-what-happens-next-16072018b.pdf.
[90] See n 24.

throughout the case law, but perhaps exemplified in the judgment of Lord Denning and Salmon and Megaw L.JJ, where, in respect of the necessity of compulsory insurance, they considered

> Parliament requires every driver to be insured against third party risks. The reason is so that a person injured by a motor car should not be left to bear the loss on his own, but should be compensated out of the insurance fund. The fund is better able to bear it than he can. But the injured person is only able to recover if the driver is liable in law. So the judges see to it that he is liable, unless he can prove care and skill of a high standard.[91]

Therefore, fault liability was seen to be moving to a system of the allocation of risk. Further, following the enactment and subsequent transposition of the Second MVID,[92] each EU Member State was required to establish a guarantee fund to satisfy claims on the basis of third-parties being injured and suffering loss due to the acts of uninsured or untraced drivers. The UK established this guarantee fund through agreements concluded between it (through the Secretary of State for Transport) and the MIB. The UK has withdrawn its membership of the EU[93] and therefore it is no longer bound by the MVID or the jurisprudence of the Court of Justice of the European Union (CJEU). Yet these are retained laws following the withdrawal and continue to have effect in the UK. This is also relevant because this is an area which the EU could seek to regulate and this could limit the choices of reform for the UK. Of course, the UK could seek to follow EU reform in this area, however this is unlikely due to the fractious relationship between the UK and EU in respect of the MVID and the UK's frequent misapplication and non-transposition of elements of the MVID.[94] Schellekens has discussed the insurance system for accidents involving autonomous vehicles.[95] He concludes that a variant of the no-fault-compensation schemes would be a feasible alternative to the liability schemes operating for conventional vehicle use. However, of course, this system is distinct from establishing a system of liability for mass-hacked CAVs given the nature of exposure to risk and the responsibility on the manufacturers to protect against such unauthorised access and modification.[96]

Establishing statutory compensation limits or minimum levels of insurance cover is perhaps not suited to motor vehicle insurance given the prospect of mass hacking and the potential consequences for an indeterminate set of claimants and an indeterminate range of losses. The insurer in these circumstances could face significant calls on them to satisfy claims with no reasonable expectation of recovering these payments from the tortfeasor (hacker). This is not to say that insurance should not be seen as a means of offering redress for the consequences of the hacking of CAVs. The MIB as a body already exists and continues to do so following the UK's withdrawal from the EU. It will also continue to contract with the Secretary of State in a similar vein to how it has done previously with the UDA and UtDA, albeit without the hindrance (as we are sure they considered it) of having to adhere to the iterations of the MVID and the jurisprudence of the CJEU. The MIB had, since its inception in the 1940's, been a source of redress, offering protection to the most vulnerable victims of road traffic accidents and using it as a compensatory body for the consequences of hacking and mass hacking of CAVs would, again reposition it as the compensatory body (indeed, as envisioned in the MVID)[97] and enable it to seize the opportunity to demonstrate its valuable existence and be able to provide a competitive advantage to road users, pedestrians and indeed any third-party victim of a hacked CAV which find themselves a victim of a motor vehicle accident caused through hacking.

---

[91] *Nettleship v Weston* [1971] 2 QB 691 [699-700].
[92] (The) Second Council Directive 84/5/EEC on the approximation of the laws of the Member States relating to insurance against civil liability in respect of the use of motor vehicles [1984] OJ LL8/17.
[93] European Union (Withdrawal Agreement) Act 2020.
[94] See James Marson, Katy Ferris and Alex Nicholson, Irreconcilable Differences? The Road Traffic Act and the European Motor Vehicle Insurance Directives (2017) The Journal of Business Law 1, 51.
[95] Schellekens (n 42).
[96] Through the establishing of technical measures for protecting the integrity of the vehicles such as by appropriate cryptography, identity authentication and remote access to the vehicle via telecommunications networks.
[97] It was in the Second MVID (The Second Council Directive 84/5/EEC [1984] OJ LL8/17) that the requirement for Member States to establish a national guarantee body (the MIB in the UK) was established.

Such positive positioning would offer reassurance to the public in the use of CAVs, to legislators to continue the compulsory insurance of autonomous vehicles and (indeed extending) the agreements established between the Secretary of State and the MIB, and with policymakers about the advantages of the UK maintaining a system of compulsory insurance with the continuation of the MIB as a national compensatory body.

As noted above, a system already exists for ensuring victims of accidents from conventional vehicles causing loss/damage in respect of the use of motor vehicles have access to compensation. Further, due to this membership a proportion of every insurance policy payment is levied to the MIB which operates the guarantee fund. EU law requires that the designated guarantee body will act as 'insurer of last resort' and provide compensation in the event that the driver of the vehicle at fault has no valid policy of insurance or who cannot be traced. The system is far from perfect,[98] the MIB frequently involves itself in claims where it is not needed,[99] and in many respects its close relationship with the insurers offering cover creates a tension in who best serves the needs of third-party victims.[100] Yet, ultimately, this system works.[101] It will now be argued that such a system will work for damage caused by vehicle hacking up to a certain limit, but would be unfit for very significant damage due to the burden placed on the insurance industry, manufacturers and ultimately the consumer. While we will distinguish the solution to the route to compensation as hacking and mass hacking we recognise that the route to compensation should not be based on whether an individual vehicle was hacked or if hacking was of more than one. An individual hack which caused significant damage could be more expensive than a fleet-based hack which applied the brakes of a few vehicles. Hence, the route to recovery should be dependent on cost rather than number of vehicles hacked.

As previously discussed, each of the other forms of redress currently available have their advantages and disadvantages for victims of accidents involving CAVs. Ultimately, however, a strategy is needed to create a system which is sustainable, fair, offers a workable mechanism for victims to be compensated in the event of injury or damage through the use of CAV, and one which also does not stifle or limit the continuing development and innovation of CAVs. Imposing liability on manufacturers for their breaches of contract, of creating defective or dangerous products is quite proper. There exist mechanisms[102] to hold such bodies liable in law and these, naturally, should continue. The difference with these situations and the consequences of hacking is for the third-party victim and their right to adequate redress and access to justice. Contract law would be of no use due to privity, and remedies in torts is problematic due to identifying the correct tortfeasor. Thus, for a low cost hack the victim should have access to a national compensatory scheme which underwrites the losses and restores the victim, as far as money can, to their previous position.

For low-cost accidents caused by hacking, we suggest that a similar model to the existing agreements between the Secretary of State for Transport and the MIB should be followed. Akin to the UDA and UtDA, a Maliciously Compromised Connected Vehicle Agreement (MCCVA), using Article 10 of the MVID as its inspiration, could provide the protection required, whilst also not placing a stifling burden on manufacturers or on insurers (as per s. 2 of the AEVA 2018). EU Member States were required, per Art. 10 of the MVID, to establish a body which would manage a fund to ensure that monies would be always available to meet unsatisfied judgments. In other words, its main role was to ensure that victims of uninsured or untraced drivers were compensated to the minimum levels of compensation to which they would be entitled to, had the driver at fault been insured/traced and the

[98] For example, see Marson, Ferris and Nicholson (n 95).
[99] *Delaney v Secretary of State for Transport* [2014] EWHC 1785 (QB).
[100] Similarly, the application of insurance to be subsumed by the manufacturer's due to their ability to generate data on risks and associated policy premiums may be disadvantageous when it comes to defects in software and hardware under their control. As has been evidenced in the popular press with accidents involving Tesla vehicles, the manufacturer has been quick to place the blame on the person behind the wheel rather than the operation of the software on the vehicle.
[101] Channon (n 39).
[102] For example, as we have discussed in terms of product liability through the CPA 1987.

claim brought against their insurer. Stipulations and exceptions were provided for in the Directive, and being an EU Directive requiring transposition into national law, there were misunderstandings and transgressions by some Member States in fulfilling the requirements of Article 10, yet overall it provided protection to a group of victims who would otherwise find themselves without a tortfeasor from which to recover compensation. The EU model provided discretion to Member States in the administration of the body (and to some extent the compensation levels applicable), but the Member States had to apply the principle of equivalence and effectiveness[103] of EU law when compensating victims under the MVID (or the aims of the Directive would be undermined – even though the UDA and UtDA both undermine these EU principles).[104] In previous articles one of the authors has criticised the UDA and UtDA, questioning whether the schemes managed by the MIB offer comparable compensation and access to protection as a claim directly against the insurer on the terms found in the policy of insurance.[105] This was a criticism of a dual system of protection which essentially saw a victim of an uninsured or untraced driver have access to compensation to a lesser degree than if they were injured by an insured and traced driver. Of course, such a scenario would not apply in our suggested system as the UK is no longer a Member State of the EU and protection for the damage and loss sustained due to the effects of a hacked vehicle would not give rise to a claim against the driver (due to lack of fault) nor should it against the insurer (given the problems with such a model as outlined above). Procedural rules could be imposed under the MCCVA so as not to deprive innocent third-party victims of road traffic accidents of their right to compensation and to ensure minimum levels of compensation are awarded. Thus, the effectiveness and equivalence principle enshrined in EU law, would be followed (simply to ensure fairness and as a benchmark to measure this by) so as not to disadvantage victims and to enable the claimant to be able to obtain the same award had they been injured by a non-hacked CAV and made an award by the insurer. The MCCVA would require all CAV to be insured or the MIB would, adopting the wording of cl 5 UDA, not be liable for any claim 'arising out of the use of a vehicle which is not required to be covered by a contract of insurance[106] unless the use is in fact covered by a contract of insurance.' This would still allow certain groups of nationally funded vehicles to be exempt as these would have the funds to call upon in the event of mass-hacking leading to damage caused by vehicles under their control - the National Health Service and the police are perhaps the most obvious examples.[107]

By establishing the MCCVA, insurers would continue to take a proportion of premiums from policyholders to supplement this fund, and, as with Pool Re (see below), at the outset of the agreement between the state and the MIB, the state would agree to underwrite compensation awards in the event that the fund was deficient. This, we argue, would only be a temporary measure and would likely not be needed to be called upon. The MIB has operated the UDA and UtDA for years through the premiums levied to it and has never been in a situation where compensation was not payable to an applicant due to lack of resources. Procedural rules on eligibility and awards would need to be established. It is beyond the scope of this paper to discuss these, although the authors have discussed the matter of procedural rules in relation to the MIB previously.[108] It is a necessary scheme,

[103] Case C-120/97 *Upjohn Ltd v The Licensing Authority established by the Medicines Act 1968 and Others* [1999] ECLI:EU:C:1999:14 at [32].
[104] See James Marson and Katy Ferris, 'Motor Vehicle Insurance Law: Ignoring the Lessons from King Rex' (2017) 38(5) Business Law Review 178 for commentary.
[105] James Marson, Hasan Alissa and Katy Ferris, 'Driving Towards a More Therapeutic Future? The Untraced Drivers Agreement and Conscious Contracting' (2021) European Journal of Current Legal Issues (in press).
[106] Per s. 144 of the RTA88.
[107] The development of the MCCVA should also be seen as a mechanism and opportunity to contract in good faith and to remove some of the more unfair and unnecessary procedural rules adopted by the MIB which, it may appear at face value, to have been included to limit the claims being made to it. For instance, the UtDA stipulates that an award is conditional on a claimant suffering personal injury from the accident in the claim, but that injury must be 'significant' in order for the MIB to proceed the claim for property damage. The result is that the value of any claims must exceed £400. This, it appears, to operate at the expense of innocent victims of untraced drivers and it would be better for the MIB to undertake a balanced assessment of its need to ensure against fraudulent claims, and its duty towards the victims of accidents.
[108] See Channon (n 39) and Marson, Alissa and Ferris (n 106).

however, as without one in place it is unlikely that truly autonomous vehicles (SAE 4-5 vehicles) will be fit for use on the road. They would simply expose the users to a liability which would be infeasible. In the next section we explore the future of insurance, and whether this is best served through a public or private scheme.

7. The future of insurance

States which have already established systems of CAVs being used and tested on public roads have done so under, typically, insurance-based schemes,[109] through the introduction of strict liability of the keeper or insurer of the vehicle,[110] or through exceptions granted under very strict circumstances.[111] These are created on the basis of facilitating the testing and limited application of CAVs on public roads, in a form of preparedness for more advanced CAV use in the future. They are not, it must be remembered, models intended as permanent solutions for more mainstream CAV use. Further, insurers could insure voluntarily for the hacking or mass hacking of a CAV as an added extra (dependent on whether this is covered under the AEVA 2018). The difficulty, however, with cybersecurity insurance, particularly cyber terrorism, is that this is an area where the risk is still very much unknown. As noted by the Cambridge Centre for Risk Studies, 'New methods for measuring cyber risk are continually adjusted, applied, and evaluated for usefulness'.[112] This is an important point. With CAV's introduction, there are a number of unknowns which the insurance model may be ill equipped to cater for. Insurance as an industry is based on actuary risk assessment. Data is taken from the applicant for a policy, and the insurer may then ascertain what premium must be paid to insure against the risk. It is not uncommon for a market to be so uncertain that a policy of insurance against the risk will not be issued. Hacking, and indeed mass hacking of fleets of vehicles operating the same software versions is an unknown quantity and this level of risk is perhaps too great to impose on the industry without a significant shift in premiums. If cybersecurity insurance is not required then increased premiums would likely mean that purchase of such insurance would be limited. If cybersecurity insurance was compulsory for vehicle users then this could mean a limited uptake of this technology.[113]

7.1 Pool / Flood Re Type Fund?

While an insurance fund based on premium income may be a positive approach for individually hacked vehicles, with an incentive maintained for both insurers and manufacturers to ensure that vehicles are cybersecure, we submit this may be problematic for vehicles which are mass hacked. This is because the potential unaffordability of insurance for consumers and the potential for insurers to be

[109] For example, the UK's AEVA 2018; Article 19 of the Italian Decree of 28 February 2018 on the testing of connected and automated vehicles on public roads (18A02619, GU n° 90 of 18 April 2018); and Spain's Directorate-General for Traffic circular of 13 November 2015 (Instrucción 15/V-113).

[110] For example, § 7 of the German Road Traffic Act (*Straßenverkehrsgesetz*) provides and continues with CAV for strict liability of the keeper of the vehicle. The French Decree n° 2018-211 of 28 March 2018 on experimentation with automated vehicles on public roads relies on the *Loi Badinter* of 5 July 1985 (n°85-677). Section 2 of the AEVA 2018 provides that 'the insurer is liable' for damage incurred by the insured or any other person in an accident caused by an automated vehicle. In the event of the vehicle being uninsured, the owner is held liable.

[111] For commentary see Stefan Nicola, Elisabeth Behrmann and Marie Mawad, 'It's a Good Thing Europe's Autonomous Car Testing is Slow' (2018) Bloomberg. https://www.bloomberg.com/news/articles/2018-03-20/it-s-a-good-thing-europe-s-autonomous-car-testing-is-slow.

[112] Cambridge Centre for Risk Studies, Cyber Terrorism: Assessment of the Treat to Insurance (2017) 31. Available at <https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/pool-re-cyber-terrorism.pdf>

[113] Studies have shown that price is potentially a significant barrier for CAV uptake. See for example Nadia Anan, Shahrina MD Nordin, Mohamad Ariff bin Bahruddin, Murad Ali, 'How Trust Can Drive Forward the User Acceptance to the Technology? In-vehicle Technology for Autonomous Vehicle' (2018) 118 Transportation Research Part A: Policy and Practice 819. Also see Zia Wadud, 'Fully Automated Vehicles: A Cost of Ownership Analysis to Inform Early Adoption' (2017) Transportation Part A: Policy and Practice 163.

unwilling to provide insurance for CAVs.[114] However, a separate reinsurance pool could be a potential solution to ensure that victims are compensated and which could limit the burden on insurers and consumers. There are a number of options here which we can explore. The first being a reinsurance pool with added state support. In this scenario insurers would provide cover up to a certain amount, and compensation required over that amount would be paid by the government (through way of a loan). The introduction of such a reinsurance pool is not novel. Pool Re,[115] was introduced in the UK for terrorism risks in 1993 after a series of terrorist attacks.[116] Reinsurers left the terrorism insurance market and Pool Re was formed to ensure that compensation could be provided through reinsurance and a government guarantee. This cover only exists in relation to commercial property damage and business interruption. Insurers cede their terrorism risk to Pool Re which then provides the necessary funds for victims. Currently, the majority of insurers in the UK contribute financially to this pool and which has built up substantial funds. Pool Re has a retrocession agreement with the government and pays a premium.[117] If pool resources do not cover the loss, the government will provide compensation, albeit as a loan which will be paid by Pool Re. Originally Pool Re did not cover for cyber terrorism, although this was later extended to cover such, although the limit to commercial property damage remains.[118] This means that commercial property damage caused by the hacking of a CAV through terrorism is already covered, although non-commercial damage and personal injury are not, nor is non-terrorism related activity. There are benefits to using a reinsurance pool compared to, perhaps, an insurance fund such as that operated through the MIB. Pool Re has funds available from itself and the government, meaning that compensation is guaranteed. The fact that insurers cover the loss, and therefore would likely recover from the manufacturer, through autonomous vehicle insurance would mean continued incentivisation of safety. However, it is worthwhile noting that the cost of such a reinsurance pool may be much more substantial than on Pool Re with the added necessity of personal injury cover, as well as the potential for an entire fleet to be hacked. This could be a much greater challenge for such a pool, both in the short and long terms due to the cost of building up funds, and repayment of the government loan, should the worst eventualities arise. In an area where the cost of insurance may already be greater at the beginning due to the cost of insuring expensive parts,[119] the added cost of such a pool may be detrimental to the uptake of CAV's due to this potential premium increase.

A similar fund in existence which could serve as a model for mass hacked CAVs, is that operated by Flood Re in respect of flood damage. We acknowledge that there are clearly differences between a government-backed scheme for compensating victims as a consequence of natural disasters and one which is established to cover harm following cyber breaches and potential cyber insecurities. Indeed, it may be a criticism levelled at the motor manufacturer industry that such harm is caused by risks introduced by industry. It is beyond the scope of this paper to detail the similarities and differences in this regard, but it is sufficient to note that several consequences of natural disasters, particularly flooding risks in the UK, have at least been impacted through private sector house building

[114] This was noted by the DfT (n 60) in terms of insurers potentially being unwilling to provide insurance if manufacturers also note the scepticism of the insurance industry in compensating for mass hacking.
[115] More information on Pool Re can be found here <https://www.poolre.co.uk>.
[116] For a definition of Terrorism, Reinsurance (Acts of Terrorism) 1993 see s. 2(2) 'In this section "acts of terrorism" means acts of persons acting on behalf of, or in connection with, any organisation which carries out activities directed towards the overthrowing or influencing, by force or violence, of Her Majesty's government in the United Kingdom or any other government de jure or de facto.'
[117] Hm Government, 'Retrocession Agreement between Pool Reinsurance Company Limited and The Lords Commissioners of Her Majesty's Treasury' (March 2015) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/417146/Pool_Re_-_Retrocession_Agreement.pdf>
[118] Pool Re, 'Introduced Remote Digital (Cyber) Cover'<https://www.poolre.co.uk/history/introduced-remote-digital-cyber-cover/>
[119] Of course, a vast reduction in accidents may reduce premiums over the longer term, however, at the beginning where the risk of CAVs is not known and the parts are expensive, it is likely that the cost will be greater.

projects.[120] Given the international standards being adopted to prevent the incidents of cyber breaches, there is precedent for the state to underwrite insurance services on the basis of public and private partnerships, irrespective of potential culpability of industry, insofar as safety standards and governmental consent to the activity is provided. As the potential for the breadth of loss as a consequence of mass hacked vehicles may therefore be akin to disaster insurance,[121] a reinsurance model operational since 2016 by Flood Re might be similarly established. Since 2000, a flood insurance partnership agreement has been in place between the Association of British Insurers and the UK government, being modified in 2007 and 2009,[122] but most radically in 2016 through the creation of Flood Re. Prior to Flood Re's formation, it had been mooted that the government may seek to begin a nationalised flood insurance system,[123] and further that this may not be restricted to flood insurance but extend to other aspects currently under the domain of the private insurance sector. Accordingly began the 'Gentleman's Agreement',[124] a cross-subsidy for at-risk property owners from the premiums paid for them and the risk-free (thus the risk was paid for by the insureds irrespective of the risk that they faced).[125] For customers, the agreement allowed everyone to be covered by insurance – business and private customers – and for the insurance sector, revenues were collected in significant numbers.

Flood Re was formed in the aftermath of several major flooding events in England and Wales which had affected the insurance industry, leading to approximately £3 billion in value of insurance claims.[126] The insurance industry considered that such scenarios were likely to increase in frequency and, consequently, the insuring against such risks would become financially unsustainable. This meant that the previous Statement of Principles,[127] upon which the agreement between the industry and government had existed, required amendment, hence the creation of Flood Re. Flood Re was designed with the aim of broadening the scope and application of affordable insurance cover to the whole population, through a process of subsidising the premiums payable by the insured, and facilitating the transition from reinsurance to the insurance sector providing cover to customers based on their risk and circumstances. Such state and industry partnership models have been identified as being beneficial[128] to ensuring continuity of insurance cover, and indeed essential where markets may be unviable in their absence.[129] Viaene and Dedene[130] extend this notion further when remarking that the '… insurance industry has positioned itself as a basic pillar of our modern society.' Yet these public-private arrangements need to be managed, as partnerships based on cover for disaster-type events often evolve over time, and the addition to and leaving of partners naturally affects the

[120] Damian Carrington 'Rush to Build New Homes will Increase Flooding, Experts Warn' (2017) The Guardian, https://www.theguardian.com/environment/2017/feb/02/rush-to-build-new-homes-will-increase-flooding-experts-warn.
[121] See Stephane Hallegatte, Economic Resilience: Definition and Measurement (2014, The World Bank).
[122] See Edmund C. Penning-Rowsell, 'Flood Insurance in the UK: A Critical Perspective' (2015) 2 WIREs Water 601.
[123] Swenja Surminski and Jillian Eldridge 'Flood Insurance in England— An Assessment of the Current and Newly Proposed Insurance Scheme in the Context of Rising Flood Risk' (2015) 10 Journal of Flood Risk Management 415.
[124] Edmund C Penning-Rowsell, Sally Priest and Clare Johnson, 'The Evolution of UK Flood Insurance: Incremental Change Over Six Decades' (2014) 30 International Journal of Water Resources Development 694.
[125] See Penning-Rowsell (n 123), 602.
[126] John Chatterton, Christophe Viavattene, Joe Morris, Edmund C Penning-Rowsell and Sue Tapsell, 'The Costs of the Summer 2007 Floods in England' (Project: SC070039/R1) (2010, Bristol: Environment Agency).
[127] Having replaced the Gentleman's Agreement in 2008 to provide for additional exclusions including the discouraging of new developments in high-risk areas by not covering such properties built after 1 January 2009.
[128] Indeed, the European Insurance industry has even identified these types of arrangements as vital in the management of risk transfer and development of prevention measures (CEA, 'Reducing the Social and Economic Impacts of Climate Change and Natural Catastrophes' (2007) vol. 46. CEA, Brussels).
[129] Colin Green and Edmund C Penning-Rowsell, 'Flood Insurance and Government: "Parasitic" and "Symbiotic" Relations' (2004) 29(3) Geneva Papers on Risk and Insurance—Issues and Practice 518.
[130] Stijn Viaene and Guido Dedene, 'Insurance Fraud: Issues and Challenges' (2004) 29 The Geneva Papers on Risk and Insurance 313, 313.

composition of the partnership and possibly has implications for its aims too.[131] For example, like many partnership models, the partners may initially have similar understandings as to the greater good that they collectively can produce, such as disaster relief and the protection against uninsured individuals, however, these shared goals may change and ultimately, the insurance sector constitutes for-profit companies which must answer to their shareholders, thereby creating potential challenges to the operation and ethos of such partnerships.[132]

How Flood Re operates in practice is through a reinsurance understanding where the state establishes a pool from which the insurance company, which provides cover to the insured, may claim in the event that the insured is affected by a flooding event. The insurance company, a private institution, offers an insurance premium to the homeowner but, as explained by Penning-Rowsell, 'if the flood risk element of the policy costs more for the company to provide than the premium set under Flood Re, that insurer can cede the flood risk part of that individual policy to Flood Re.'[133] The pool is funded through a levy[134] on all the insurance companies in the market (set for the first five years of its existence at £180 million but reviewed thereafter) and, significantly for the purposes of our proposed modelling of a similar structure against the mass hacking of CAVs, it was established for a life of 25 years.[135] During this 25-year term, alternatives to Flood Re would be put in place to remove the need for a central government fund (as insurer of last resort)[136] from which reinsurance could be purchased.[137]

Having briefly described the reinsurance models which we propose as a solution to an impending threat to the safety and viability of CAV use in the UK, it is important to examine the criticisms that exist for such models so they can be addressed from the outset and considered with the benefit of hindsight and of having seen the operation of these schemes. Flood Re is the focus here, for reasons explained above as to the symmetry between floods and hacked CAVs in respect of numbers of affected parties (first and third-parties) and the 'disaster' potential for such events. We also feel this is a useful exercise given that it would be reasonable to conclude that Flood Re's existence has been subject to strong criticism on a number of bases.

Many of the academic and professional commentary in this respect overlap, but if we begin with Penning-Rowsell, he identifies issues with the creation of Flood Re itself which is predicated on the

[131] Florence Crick, Katie Jenkins and Swenja Surminski, 'Strengthening Insurance Partnerships in the Face of Climate Change – Insights from an Agent-based Model of Flood Insurance in the UK' (2018) 636 Science of the Total Environment 192.

[132] See Crick, Jenkins and Surminski (n 132); Coliin Armistead, Paul Pettigrew and Sally Aves, 'Exploring Leadership in Multi-sectoral Partnerships' (2007) 3 Leadership 211; Justine Chen, Ted Hsuan Yun Chen, IIan Vertinsky, Lilia Yumagulova and Chansoo Park, 'Public-Private Partnerships for the Development of Disaster Resilient Communities' (2013) 21(3) Journal of Contingencies and Crisis Management 130; and Swenja Surminski and Hayley Leck, 'You Never Adapt Alone – The Role of Multi-Sectoral Partnerships in Addressing Urban Climate Risks' (2016) Centre for Climate Change Economics and Policy Working Paper No. 262. Grantham Research Institute on Climate Change and the Environment Working Paper No. 232. London.

[133] See Penning-Rowsell (n 123), 603-4.

[134] Insurers pay an estimated £10.50 per policy (a highly-discounted price available through Flood Re) which may be passed on to policyholders (estimated to be £10.50 per policy (Aviva, 'Half Year 2016 Earnings Presentation – Final' 2016).

[135] Per Flood Re 'Flood Re has been designed to provide temporary support to the insurance market for properties at high risk of flooding. At the end of 25 years from the date the Water Act 2014 received Royal Assent (May 2014), Flood Re will have been wound up and the subsidy provided through the scheme removed.' Flood Re. (2016) 'Transitioning to an Affordable Market for Household Flood Insurance: The First Flood Re Transition Plan' http://www.floodre. co.uk/wp-content/uploads/Flood-Re- Transition-Plan-Feb-2016-FINAL.pdf.

[136] Michael Huber, 'Insurability and Regulatory Reform: Is the English Flood Insurance Regime Able to Adapt to Climate Change' (2004) 29 The Geneva Papers on Risk and Insurance 169.

[137] Department for Environment, Food and Rural Affairs (Defra), 'A Short Guide to Flood Re' (2014, London: Defra) https://consult.defra.gov.uk/ flooding/floodreinsurancescheme/supporting_documents/ A%20short%20guide%20to%20Flood%20Re.pdf.

perceived unfairness of the system as a mechanism for insurance against risk and the problem with reinsurance models. Insurance is purchased by individuals on the basis of perceived risk, who spread this risk across the payment of premiums over a period of time rather than taking the risk of suffering substantial losses due to episodic events. However, the nature of Flood Re involves the majority of insureds paying premiums containing a levy which subsidizes those at much greater risk and who are more likely to claim on their insurance policy. This is problematic given that many individuals purchasing insurance will not be aware of the proportion of their premium being used explicitly for the purpose of covering more 'at risk' policyholders. This is a point returned to later, but it is sufficient at this point to remark that what is evident from this model is that many individual persons and businesses, due to their lack of understanding of the existence and operation of the levy, will have no awareness or incentive to change their behaviour / make alternative provision to reduce their future risk, in respect of the risk their current circumstances place them in. It is important to note at this stage the necessity of such reinsurance schemes to account for shortcomings in the insurance sector which, save for the existence of the reinsurance system, would expose too many individuals to risks for which they are unable to insure against. It is also important that this includes governmental backing as, being explained by Green and Penning-Rowsell,[138] state-inclusive partnerships are necessary to ensure public acceptance and confidence of such schemes. Yet this too creates an important issue which requires consideration for future schemes. The stakeholders (government, insurance industry, property developers, property owners and so on) are involved and affected by the reinsurance arrangement having been established,[139] yet several of these have no direct link or involvement in its running and/or strategic decision-making. Further still, this insurance model cannot be maintained indefinitely unless the underlying issues which led to its conception are not addressed, and reinsurance models have been accused of, potentially, actually working against the partnership's higher aims.[140]

State-backed reinsurance structures are also less able to diversify across different perils and are typically slower to adapt to different scenarios, thus being seen as less flexible.[141] Nor does a reinsurance pool promote behavioural change or the establishing of a portfolio of measures to encourage, for instance, risk-reducing behaviour.[142] Indeed, for Winter,[143] this can institute instances of moral hazard and even situations where property holders' actions might increase the probability and size of their loss.[144] Insurance has even been used, claim some academics,[145] as a disaster risk management tool for the influence of policy-makers and planning authorities. Studies, such as those

[138] Green and Penning-Rowsell (n 130).
[139] Summarised as being '… not simply a question of engineering; it is a rather complex area, with political, economic, social and environmental dimensions'. Swenja Surminski and Jillian Eldridge, 'Flood Insurance in England – An Assessment of the Current and Newly Proposed Insurance Scheme in the Context of Rising Flood Risk' (2017) 10(4) Journal of Flood Risk Management 415, 415.
[140] Crick, Jenkins and Surminski (n 163), 194.
[141] Penning-Rowsell (n 123), 606.
[142] EP Evans, R Ashley, Jim Hall, Edmund C Penning-Rowsell, Paul Sayers and CA Thorne, 'Foresight Future Flooding: Scientific Summary. Volume I: Future Risks and Their Drivers' (2004, Office of Science and Technology, London); and EP Evans, Jim Hall, Edmund C Penning-Rowsell, A Saul, Paul Sayers, CR Thorne and AR Watkinson, 'Drivers, Responses and Choices for Future Flood Risk Management' In: Proceedings of ICE, Water Management 159, March 2006, 53.
[143] Ralph Winter, 1992 'Moral Hazard and Insurance Contracts' in Georges Dionne (ed) Contributions to Insurance Economics (1992, Huebner International Series on Risk, Insurance and Economic Security, Boston MA).
[144] Howard Kunreuther, 'The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage Risk' (2002) 22 Analysis 427; and Sally J Priest, Michael J Clark and Emma J Treby, 'Flood Insurance: The Challenge of the Uninsured' (2005) 37(3) Area 295.
[145] David Crichton, 2008. 'Towards a Comparison of Public and Private Insurance Responses to Flooding Risks' (2008) 24 International Journal of Water Resource Development 583; Swenja Surminski, 'The Role of Insurance in Reducing Direct Risk - The Case of Flood Insurance' (2014) 7(3-4) International Review of Environmental and Resource Economics 241; and Swenja Surminski, Jeroen Aerts, Wouter Botzen, Paul Hudson, Jaroslav Mysiak and Carlos Perez-Blanco, 'Reflections on the Current Debate on How to Link Flood Insurance and Disaster Risk Reduction in the European Union' (2015) 79 Natural Hazards 1451.

just previously noted,[146] have reported that the purchasing of, extending even to merely the ability to purchase, insurance cover can influence the behaviour of those subject to the risk. This has been witnessed positively[147] through the development of preventative measures as a means to reduce risk.[148] However, it might also reduce the government's incentives to prevent and reduce the cause of the risks in question given it reduces the governmental intervention needed following a major flooding event.[149]

Thus, this is not just about individuals managing their own risk and adopting behaviours to mitigate against the worst effects, it is also about the industry itself preparing for the ending of the partnership. As noted above, when established in 2016, Flood Re was designed to exist for a 25-year period, the end of which would see the insurance industry provide the coverage for flood susceptible properties through actuary risk assessment and management. Yet the current Flood Re partnership is opaque, does not clearly identify risk and reflect this in the pricing of policies, and thus fails to establish the forward-planning necessary for the consequences facing all parties at the end of the partnership. At present, the main beneficiaries to the Flood Re arrangement are the insurance companies and their shareholders, along with property owners who would otherwise find themselves paying significant premiums for cover against the substantial risk from flood damage. There is seemingly no plan for the ending of the relationship and the transition to affordable, available and risk-reflective insurance policy pricing.[150] Nor are there specific mechanisms in place to determine its efficiency, efficacy, fairness and advantages in promoting good behaviour.[151]

Certainly, some of the most critical points (and a very thorough review) of Flood Re has been provided by Christophers.[152] The arguments he presents are particularly relevant considerations when seeking to prevent similar 'problems' being encountered with the creation of a 'new' reinsurance fund to accommodate mass hacked CAVs. First, where a reinsurance fund is created for a fixed time period (say 25 years – akin to Flood Re), it should not be simply expected that the market will naturally metamorphosize and develop a risk-based approach which will be ready to take over the service offered through the previously administered insurance guarantee fund. Such a presumption[153] that a market will automatically follow from the reinsurance fund '… is merely symbolic, figurative. Alluded to rather than actively delineated… in sum, allusive.'[154] Perhaps most damning is his contention that 'insisting that a market for flood insurance is possible, and alluding to its future crystallization, serves to obviate the need for pursuing in the here-and-now sustainable, non-transitory, non-market-based approaches to flood risk management.'[155] This criticism may be harsh, even too harsh, and there are distinctions we can draw between Flood Re and a fund for mass hacked

[146] ibid.
[147] Although perhaps underutilized, see Jessica Lamond, David Proverbs and Felix Hammond, 'Accessibility of Flood Risk Insurance in the UK: Confusion, Competition and Complacency' (2009) 12 Journal of Risk Research, 825; and Swenja Surminski and Paul Hudson, 'Investigating the Risk Reduction Potential of Disaster Insurance Across Europe' (2016) 42 Geneva Papers on Risk and Insurance - Issues and Practice 247.
[148] Wouter Botzen and Jeroen van den Bergh, 'Managing Natural Disaster Risks in a Changing Climate' (2009) 8 Environmental Hazard 209; Howard Kunreuther and Erwann Michel-Kerjan, 2009. 'Managing Catastrophes Through Insurance: Challenges and Opportunities for Reducing Future Risks' Working Paper 2009-11-30. The Wharton School, University of Pennsylvania, Philadelphia; and Emma Treby, Michael Clark and Sally Priest, 'Confronting Flood Risk: Implications for Insurance and Risk Transfer' (2006) 81 Journal of Environmental Management 351.
[149] Huber (n 137).
[150] Johanna Hjalmarsson and James Davey, 'Flagship Plan to Rescue Flood-hit Home Owners Already Looks Out of Its Depth' (2016) The Conversation http://theconversation.com/flagship-plan-to-rescue-flood-hit-home-owners-already-looks-out-of-its-depth-52791.
[151] This being left to commentators – see, for instance, Penning-Rowsell (n 154), 601.
[152] Brett Christophers, 'The Allusive Market: Insurance of Flood Risk in Neoliberal Britain' (2019) 48(1) Economy and Society, 1.
[153] What Butler has referred to as 'market presumption.' Judith Butler, 'Performative Agency' (2010) 3(2) Journal of Cultural Economy, 147.
[154] Christophers (n 153), 2-3.
[155] Christophers, (n 153), 4.

CAVs, but it is a point worth noting and considering. There is strong evidence of active and substantial work to (cyber) secure vehicles, not just on a national level but internationally too. Further, these cybersecurity requirements (as noted above) have also found their way into legislative instruments and are being 'baked into' CAV software development. This does not negate the argument for a central guarantee fund being present, rather it seeks to explain how the government in the UK is not obviating its role in seeking to prevent cyber breaches, and is perhaps being more assertive in cybersecurity for the introduction of CAVs than it might have been to manage regional flood defence systems and tackle the much more significant issue and effects of climate change. A reinsurance arrangement for the protection of all parties in the burgeoning CAV market would benefit the market itself and allow it space to develop and understand the intricacies of changes to vehicle use and the interactions between software, hardware and end-user experience, with the wealth of data being generated which could be harnessed for actuary risk assessment (as with Tesla's tentative move into the insurance sector)[156] until that market is ready to take over insurance cover.

This will mitigate against the argument levelled against Flood Re by many academics and commentators that key actors are unlikely to be incentivised to change their behaviour in respect of risks and the insurance landscape will remain static and not seek to assess risk more accurately to accommodate the transition away from reinsurance systems. The disconnect between the risk (here of flooding) and the management of insurance costs and claims outside of Flood Re, as noted by Christophers,[157] is less likely with a CAV reinsurance model. A major criticism of Flood Re is that data is shared between the state and the insurers in the industry, and its existence and the temporality of this existence, was not shared more broadly to individuals within the market. These can be avoided with the sharing of information, and informing users who can be proactive in managing their own risk over the, say 25 years, of the life of the CAV reinsurance scheme. This might include their choosing manufacturers with good cybersecurity systems, understanding the need for CAV software support and considering the regularity of such safety updates, the reliability of on-board internet connectivity, understanding how their data could be used to determine risk (given the previous models for car insurance will be largely redundant with vehicles which drive without human interaction) and so on. This information sharing had been requested by Lord Krebs in 2014 in respect of Flood Re,[158] but ultimately it was restricted between the state and the insurers (perhaps a mistake, albeit one which is not incapable of being rectified).

The above criticisms, albeit applied to Flood Re, are not, ultimately, faults of its creation but rather of the system established by the government. The remit of Flood Re to facilitate a transition to a market-led structure of cover was ultimately hamstrung, for, as observed by Bek,[159] 'The fundamental tools to create an environment for risk reflective pricing lie with the government and not with Flood Re.'[160] This point was also made by Christophers when he notes the '… fundamental mismatch between Flood Re's powers on the one hand and its responsibilities on the other. The government has simply not given Flood Re the tools it would need to have any chance of getting the long-term job done.'[161] Indeed, such criticism is not restricted to the academic community. In the Commons, Barry Gardiner considered that the government had not issued Flood Re with responsibilities, instead it had abdicated its responsibility.[162]

[156] Alex Zarifis, 'Why is Tesla Selling Insurance and What does it Mean for Drivers?' (31 January 2020) The Conversation https://theconversation.com/why-is-tesla-selling-insurance-and-what-does-it-mean-for-drivers-130910.
[157] Christophers (n 153), 19.
[158] HL Deb 11 February 2014, c586.
[159] Mateusz Bek, 'Flood Re: Together, Though not all and not Forever' (2015) In Johanna Hjalmarsson (ed) Future Directions of Consumer Flood Insurance in the UK: Reflections upon the Creation of Flood Re https://eprints.soton.ac.uk/380346/1/58175_ Report_v4_WEB.pdf.
[160] Bek (n 191), 38.
[161] Christophers (n 153), 22.
[162] HC 27 October 2015, c7.

When accepting the criticism levied at the Flood Re partnership, there are notable successes and differences between a reinsurance fund for flood risk areas, and the external factors, climate change not least of these, which exist which would be less likely to affect mass-hacked CAVs. For example, the potential deficiencies raised by Christophers,[163] Crick, Jenkins and Surminski,[164] Green and Penning-Rowsell,[165] Surminski[166] and others noted in our critique, of failures to incentivise flood risk management and risk reduction efforts (through the subsidizing of premiums), of reducing the economic inefficiency of the Flood Re model, and so on, would likely to be less applicable to CAV manufacturers given their control of the environment in which these vehicles are manufactured and operate, and because of the control over the extent to which such extreme failures can spread between connected vehicles. In respect of Flood Re, it lacks a scheme for building capacity for risk reduction; has no compulsory system of risk reduction; and has limited commitment from government to do more in reducing flood risks.[167] The government is committed to being a leading player in the design, development and deployment of CAVs and therefore its various layers of governance appear to possess a cohesive aim in shaping insurance (through compulsory cover, providing an enabling infrastructure, through adherence to international codes and risk reducing schemas and so on) to make viable CAV use in the UK. Consequently, while similar broad arguments as above might have been levied against the stakeholders in the event of mass hacked CAVs, the CAV reinsurance scheme, insurers and the government would be able to liaise with manufacturers to manage the risk factors whilst Flood Re has little direct communication or influence to facilitate change with policyholders. Flood victims also need various stakeholder engagement (banks, local authorities, developers, architects and so on) for risk reduction which would not apply in the context of CAVs. The transparency of premiums needs to be managed so, whilst they may be approximately similar across all CAV users, risk management must be a feature which enables an effective transition to when the government / insurance industry partnership against mass hacking comes to an end. Part of this transition will require insurers to, compulsorily, identify and reduce premiums where safety systems are in place which actively reduce risk, irrespective of the additional costs involved when investigating the risk circumstances of potential customers / car and software manufacturers. The powers provided to the Secretary of State for granting the status of CAVs in the AEVA 2018 will also allow it to manage certain data regarding accidents, software updates, safety records and so on. These data will address much of the information vacuum present in the Flood Re arrangement.

Ultimately, the model devised for Flood Re, whilst flawed, does appear to work and benefits stakeholders in respect of the overarching aims of its creation. As evidenced by Dubbelboer et al.[168] through their analysis and modelling, Flood Re has been shown to reduce premiums to accessible levels (halving the expected costs in premiums over a 30-year period), whilst also changing developer practices of building on land susceptible to surface water flooding to reduce risk and suggesting that the Flood Re model '… is capturing the main function of the scheme correctly.'[169] Similar sentiments are offered by Priest et al., who acknowledge the insurance protection offered through Flood Re's creation, and continue that this alliance makes it probable that the partners would aim to reduce future vulnerabilities and the likelihood of it having to, once again, provide financial assistance to the market.[170]

Thus, an alternative solution would be for the government to take on much more of the risk, and fund perhaps a majority of the cost from mass-hacks. This could be through not requiring any government

[163] Christophers (n 153).
[164] Crick, Jenkins and Surminski (n 163),
[165] Green and Penning-Rowsell (n 161).
[166] Swenja Surminski, 'Fit for Purpose and Fit for the Future? An Evaluation of the UK's New Flood Reinsurance Pool' (2018) 21(1) Risk Management and Insurance Review 33.
[167] Surminski (n 167), 53.
[168] Jan Dubbelboer, Igor Nikolic, Katie Jenkins and Jim Hall, 'An Agent-Based Model of Flood Risk and Insurance' (2017) 20(1) Journal of Artificial Societies and Social Simulation 6.
[169] Para 4.5.
[170] Sally J Priest, Michael J Clark and Emma J Treby, 'Flood Insurance: The Challenge of the Uninsured' (2005) 37(3) Area 295, 300.

assistance to be paid back or simply for the government to provide compensation through a separate fund. This solution therefore is essentially one of public v private (or a mixture of both) i.e. whether the consumer (and other insureds due to the loss spreading nature of insurance) or the taxpayer should have the ultimate burden of compensating. Whilst insurance is a loss spreading device,[171] spreading the cost of mass hacking through taxpayers would spread this much further and potentially to a wider pool of people. Of course, in the most catastrophic of instances of damage, government resources could be severely strained.[172] It is likely that given the uncertainties above, and the differences in compensation for damage through terrorism activities (relatively small) compared with those involving the use of CAVs (injuries involving motor vehicles being, comparatively at least, quite commonplace), a governmental-backed guarantee fund may be the more effective, known and easily-implemented model, at least at the outset. Following an evaluation of CAV roll-out, risk trends and loss events, the model could be subject to re-evaluation and a fitness for purpose test.

8. Conclusion

CAVs have the potential to fundamentally affect public and private forms of travel. The change that level 5 SAE vehicles will bring will be unlike anything witnessed on public roads before and has the potential to benefit and provide mobility access to a range of stakeholders. The connected nature of the vehicles is their strength and their weakness. The rolling out of 5G networks will ensure that the real-time information and data sharing necessarily underpinning CAV infrastructure will facilitate the communications and AI for their operationalisation. Software updates will be an essential component of their deployment and use, these will happen over-the-air and with regularity, and this will enable those with malicious intent to hack the software, with potentially catastrophic consequences. Without appropriate insurance systems, CAVs could pose too great a danger to road users if the vehicles suffered serious software defects or, as we focus on in this paper, were subject to malicious hacking. We have outlined the currently available liability systems to facilitate CAVs' introduction onto public roads and outlined their deficiencies or inapplicability to vehicles which operate without a driver in control. There exist two main methods to ensure third-party victims of accidents involving these vehicles have access to minimum standards of compensation and redress. The first noted operates through a public guarantee fund. This, following a presently established model operated in a series of agreements between the state and the MIB, would protect the public and users of CAV, remove a potentially onerous burden on manufacturers and the insurance industry, and would enable the deployment and advancement of CAVs in the UK. The second method is more 'private' in nature where the government and the insurance industry operate a scheme similar to those in Pool Re and Flood Re. Whichever model is chosen, and given that the UK was the first state to introduce (prospective) legislation to regulate the insurance of CAVs, it would be fitting for the UK to lead the way in establishing a guarantee fund to provide the certainty to all parties on the placement and use of CAVs, and thereby facilitating the advancement of the CAV industry.

[171] See Rob Merkin and Jenny Steel, Insurance and the Law of Obligations (2015 Oxford University Press) which analyses in detail the role of insurance in loss spreading.
[172] Anne Gron and Alan Sykes, 'Terrorism and Insurance Markets: A Role for the Government as Insurer?' (2003) 36 Indiana Law Review 447.