www.jusletter-it.eu

Jonathan Sinclair / Burkhard Schafer

Autonomous Vehicles: The Path to Liability is Still Unclear

Governments are scrambling to support innovation and pre-empt societal expectations, no more so than in the emerging domain of autonomous vehicles. This publication will address one countries (UK) approach towards legal liability, assess the proposition being put forth and highlight key concerns that question the pragmatic approach being presented. A case will be made against defaulting to a model of strict liability and insurance, suggesting that the possibilities of external manipulation (car-hacking) and the very nature of dynamic machine learning algorithms prove obstacles in assigning accountability.

Category: Articles
Region: Switzerland
Field of law: AI & Law

Citation: Jonathan Sinclair / Burkhard Schafer, Autonomous Vehicles: The Path to Liability is Still Unclear, in: Jusletter IT 23 November 2017

Contents

1. Introduction: Setting the Scene

[Rz 1] You're standing in front of your house, coffee in hand, waiting for your car to pick you up. While driving through a residential area, you receive a message on your console stating: «Your car has been taken over by Anonymous, pay now or face the consequences», you decline, assuming a hoax, then suddenly realise that your car isn't responding any longer. At this point it starts to accelerate aiming at pedestrians on the pavement. Nothing you try averts the cars course of action, your car then drives into a busy restaurant injuring customers and yourself.

[Rz 2] A nightmare or science fiction? With the advent of automated vehicles this has now become a possible scenario. Indeed, first exemplar cases have already been reported[1].

[Rz 3] For the UK, the recent proposal by the Department for Transport (DoT) touches upon the issue of driver liability in a world of hackable autonomous vehicles, but only in passing[2].

[Rz 4] This paper will build on this discussion and demonstrate that, while it identifies a solution to some of the legal implications surrounding autonomous driving, other aspects require further thought and ultimately, additional changes to the existing legal instruments will be required.

2. The Legal Framework

[Rz 5] Autonomous vehicles are on the march[3] and there seems little stopping the encroachment of robotic agents into our daily lives. Both the government and private sector are making conservative estimates that levels 4 and 5 of autonomy (referencing complex driving situations and

1 Andrew J. Hawkins, Uber says it's reviewing incident of self-driving car running a red light, The Verge, 14 December 2016, available at: http://www.theverge.com/2016/12/14/13960836/uber-self-driving-car-san-francisco-red-light-safety (all websites last accessed on 16 November 2017); Evan Ackerman, Fatal Tesla Self-Driving Car Crash Reminds Us That Robots Aren't Perfect, Spectrum, 1 July 2016, available at: http://spectrum.ieee.org/cars-that-think/transportation/self-driving/fatal-tesla-autopilot-crash-reminds-us-that-robots-arent-perfect.

2 Department for Transport, Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies, 2016, available at: http://webarchive.nationalarchives.gov.uk/20170123080341/https:/www.gov.uk/government/uploads/system/uploads/attachment_data/file/536365/driverless-cars-proposals-for-adas-and_avts.pdf.

3 With some figures estimating that 10 million cars that possess some form of driving automation will be on the road by 2020; see: BI Intelligence, 10 million self-driving cars will be on the road by 2020, Business Insider Deutschland, 15 June 2016, available at: http://uk.businessinsider.com/report-10-million-self-driving-cars-will-be-on-the-road-by-2020-2015-5-6.

full, end-to-end, hands-off journey autonomy) will be achieved somewhere between 2020 and the 2030's[4].

[Rz 6] With the onset of this automation into our daily lives and into an environment that already carries an accepted risk profile[5], a large number of legal and societal questions are brought into focus.

3. Background

[Rz 7] Technological advancement in this space isn't new. Research in this area has been actively performed since the 1920s[6], but legal and regulatory bodies were slow to address the issue outright, no doubt due to the public's unwillingness to entrust its safety to a machine, and as a result of pragmatic hurdles surrounding battery, sensor and computational technologies.

[Rz 8] In 2011, things started to change with the United States (US) drafting legal instruments to cope with the onset of autonomous vehicles, initially by the state of Nevada[7], followed by subsequent states, until today, where 16 states[8] have either enacted, or are looking to enact, legal policy and regulatory measures to allow for autonomous vehicles to exist alongside normal, human operated motor vehicles. This change is being reflected globally with prominent countries following suit such as the UK, Japan and Singapore[9].

[Rz 9] From the periphery, it would appear that everything is developing well, new technology is being adopted, supported by legislative evolution, under the premise that everyone will be driven by autonomous agents come 2021[10], increasing safety, reducing human error and allowing productive use of time when in transit.

[Rz 10] However, legal solutions are still suffering from gaps, when considering the proposals mentioned in the 2016 DoT paper[11], with problems associated around liability, accountability, ethics and legal codification emerging, undercutting the optimistic outlook.

---

4 KPMG, Connected and Autonomous Vehicles – The UK Economic Opportunity (2015), available at: https://www.smmt.co.uk/wp-content/uploads/sites/2/CRT036586F-Connected-and-Autonomous-Vehicles-%E2%80%93-The-UK-Economic-Opportu...1.pdf.

5 Department for Transport, UK Annual road fatalities (2014), available at: https://www.gov.uk/government/publications/annual-road-fatalities#history.

6 Adrienne Lafrance, Your Grandmother's Driverless Car, The Atlantic, 29 June 2016, available at: http://www.theatlantic.com/technology/archive/2016/06/beep-beep/489029/.

7 Nevada state AB 511 legislature approval, 28 March 2011, available at: http://www.leg.state.nv.us/Session/76th2011/Reports/history.cfm?ID=1011; Assembly Bill No. 511–Committee on Transportation, 2011, available at: http://www.leg.state.nv.us/Session/76th2011/Bills/AB/AB511_EN.pdf.

8 National Conference of State Legislatures, Autonomous self-driving vehicles legislation, 2016, available at: http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx.

9 Charlotte Jee / Christina Mercer, Driverless car news: The great driverless car race: Where will the UK place?, Techworld, 22 June 2017, available at: http://www.techworld.com/personal-tech/great-driverless-car-race-where-will-uk-place-3598209/.

10 Reuters, BMW says self-driving car to be level 5 capable by 2021, Reuters UK, 16 March 2017, available at: http://uk.reuters.com/article/uk-bmw-autonomous-self-driving-idUKKBN16N1Y8?il=0.

11 DoT, Pathway to Driverless Cars 2016 (note 2).

4. State of the Art

[Rz 11] Car hacking, and the issues this activity raises are becoming a seriously discussed topic. Since 2015, with the advent of the infamous Jeep Cherokee case involving security researchers Charlie Miller and Chris Valasek[12], it's one that is attracting serious attention, with the aforementioned security exploit resulting in the recall of 1.4 million cars by Fiat[13] and resulting in the US National Highway Traffic Safety Administration opening an investigation into the recall.

[Rz 12] Since this time, Miller and Valasek have continued their research, uncovering further issues with the underlying systems[14] of the same vehicle, while researchers in China have identified issues with other car manufactures systems e.g. Tesla[15]. While commentators such as David Pogue, of Scientific America, attribute these developments to scare mongering tactics[16], the fundamental job of regulators and law makers is to attempt to pre-empt technological advances and ensure the legal landscape is prepared to deal with these new issues, even if, at present, the threats and risks may be arbitrarily «hypothetical». The inauguration of a «Car hacking village» (2015) at the world's leading hacker event Defcon, would suggest these «hypothetical» issues will become non-hypothetical very soon.

5. Legal Treatment

[Rz 13] The DoT UK report provides legal mechanisms for dealing with a number of tricky legal areas, proposing that answers can be found by way of «a proportionate response», passing the «duty of care» onto car manufacturers and insurance companies, stating the following as a key strategic driver:

> «*Our proposal is to extend compulsory motor insurance to cover product liability to give motorists cover when they have handed full control over to the vehicle (i.e. they are out-of-the-loop). And, that motorists (or their insurers) rely on courts to apply the existing rules of product liability – under the Consumer Protection Act, and negligence – under the common law, to determine who should be responsible.*»[17]

[Rz 14] This delegation of responsibility onto industry is a pragmatic approach and as long as industry identifies that commercial gains outweigh the risk,[18] and traceability of liability is clear, one could believe that this approach would work.

---

12 Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway – With Me in It, Wired, 21 July 2015, available at: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

13 David Shepardson, Fiat Chrysler will recall vehicles over hacking worries, The Detroit News, 24 July 2015, available at: http://www.detroitnews.com/story/business/autos/2015/07/24/us-pushing-guard-vehicle-cyberhacking/30613567/.

14 Andy Greenberg, The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse, Wired, 1 August 2016, available at: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

15 Andy Greenberg, Tesla Responds to Chinese Hack With a Major Security Upgrade, Wired, 27 September 2016, available at: https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/.

16 «Yes, new technology is always a little scary. But let's not exploit that fear. Let's assess the hackable-car threat with clarity, with nuanceand with all the facts»; see David Pogue, Why Car Hacking Is Nearly Impossible, Scientific American, 28 October 2016, available at: https://www.scientificamerican.com/article/why-car-hacking-is-nearly-impossible/.

17 DoT, Pathway to Driverless Cars 2016 (note 2), p. 12.

18 As in the case of the financial sector e.g. credit card forgery and embezzlement etc.

6. Issues with Liability

[Rz 15] If insurers and manufactures agree to the recommendations put forth by the DoT, questions must be asked regarding scenarios which may obscure liability, e.g. if an autonomous vehicle is externally manipulated, does the owner remain liable for what happens and if so, are they covered by their insurance?

[Rz 16] The DoT paper addresses this problem, and suggests to treat car-hacking as the equivalent to car-hijacking, as a normative equivalent to a theft of the vehicle. *How* the car is brought under the control by a third party does not matter – by breaking the door or by breaking code – as long as the result is the same. This however plays down the special nature of cyberspace, where accountability and traceability is not a given.

> «*If an accident occurred as a result of an automated vehicle being hacked then we think it should be treated, for insurance purposes, in the same way as an accident caused by a stolen vehicle. This would mean that the insurer of the vehicle would have to compensate a collision victim, which could include the «not at fault driver» for damage caused by hacking but, where the hacker could be traced, the insurer could recover the damages from the hacker.*»[19]

[Rz 17] One problem with this approach is that it does not unpack sufficiently what «hacking» in this context means, and the forms it can take. To illustrate this, we can imagine a range of scenarios, derived from the legal concept of theft, that aid to obscure the pragmatic approach to this dilemma e.g.

[Rz 18] In particular we can distinguish scenarios where someone manipulates your autonomous vehicle and:

1) Takes full control of the vehicle. It now responds to the hacker in exactly the same way as it would to the «driver»
2) Obtains marginal control over some functions, but not direct control over the entire car: For instance, they can increase or decrease speed, but not influence the direction
3) Does not control these functions, but interferes with and degrades the performance of the software, eventually resulting in an accident e.g. the brakes are less responsive, or reaction to external obstacles slowed down. The will of the driver is thwarted (the driver wants to slow down, but can't) but neither is the hacker now in control
4) Uses ransomware to «hold it hostage». In this case, the malicious intruder can't manipulate the vehicles functions but then neither can the owner. The hacker exercises a degree of control at the detriment of the lawful owner, and it is in their power alone to restore full access. It is at least debatable if this is best understood as theft, or as criminal damage combined with extortion. In this scenario, it is unlikely (because the vehicle is now incapable of movement) that accidents occur, but also not impossible – e.g. if the car is disabled in an unsafe space and could not be physically moved before a third party ran into it.
5) Disrupts the information the vehicles control system is receiving e.g. manipulation of the speedometer, causing the driver to behave incorrectly, resulting in incurring civil or criminal penalties. This differs from the previous scenario in that here, a human driver is again involved, so arguably an issue only for level 4 automation and below

19 DoT, Pathway to Driverless Cars 2016 (note 2), p. 21.

6) Manipulates the core decision making algorithms e.g. machine learning, rule based decision trees etc. and feeds these false information, resulting in sensor manipulation directly affecting the vehicles behaviour. In this scenario the attacker does not directly exercise control, but neither does the owner. In this scenario, the behaviour of the car is less predictable than in 2 or 3 – for anyone, including the hacker.

[Rz 19] The first two scenarios are closer to the concept of theft as traditionally understood, and raise similar issues were an accident to occur. The other scenarios, in varying degrees, look more like vehicle damage where the theft analogy appears to break down and does not seem appropriate. The question then is if the DoT really wants to treat all hacking cases alike, as the equivalent of theft (the literal reading of the proposal) or if it only had the «prototypical» scenario 1 in mind, and treat scenarios 3-6 like third party damage to the car that impedes its road safety. In this case, clarification would be needed just how much control a hacker has to exercise before they can be deemed to be in control of the vehicle, and thus «stealing» it. From the perspective of third party victims of an accident however, this distinction would not make a difference in practice.

[Rz 20] Orthogonal to this issue is the duty, if any, of the owner to prevent these attacks from occurring. Unlike some jurisdictions, in the UK, theft breaks the chain of responsibility for the stolen car absolutely, even though the owner contributed through their negligence to the theft. On the other hand, their insurance remains liable for the damage the thief caused, though if the thief was identified and has assets, an action for recovery against them is possible.

[Rz 21] From a policy position, it could be debated if this gives the right incentives to owners to protect the software of a car against hacking. The worst they face is an increase of their premiums, but they are shielded from criminal and personal civil liability, while their insurance covers the damage to third parties. This is in line also with other parts of the DoT proposal. It specifically proposes that third party claims can be made against drivers who negligently kept the computer software in a vulnerable state, even if this is against the terms and conditions of their insurance contract. Or put differently, a car does not become uninsured merely because the owner «fails to properly maintain and update the AVT (automated vehicle technology) or attempts to circumvent the AVT in breach of their insurance policy».

[Rz 22] This approach may be what is needed to reassure the public and increase acceptance of automated vehicles. While we may intuitively feel that the scenarios 1-6 mentioned above lump too many different categories together, the ultimate outcome achieves the desired end. It also replicates in its results, as far as third parties are concerned.

[Rz 23] From the insurance industry perspective too, this solution looks initially promising. Unlike the «first party» insurance model that the DoT considers briefly and rejects, it still allows them to price their product based on the accumulated experience with individual cars and individual owners[20]. It also allows them, again through the way premiums are calculated, to exercise an element of control over the costs, e.g. by giving owners reductions for theft prevention technology. It is however at this point that the cybertheft scenario and the traditional theft diverge. In traditional theft, thief and stolen vehicle must be in close proximity, and even the most aggressive or talented of thieves will only ever been able to steal a limited number of cars. This means the total number of car thefts at any given moment in time stays a small percentage of all the cars on the

[20] DoT, Pathway to Driverless Cars 2016 (note 2), p. 23.

road, and of those stolen, only a few will ever be involved in accidents that harm third parties. This enables insurance companies to quantify the associated risk – a risk which they then can further diminish, as discussed by incentivising anti-theft devices through reduced premiums.

[Rz 24] For some forms of car hacking, this will remain the case. In particular in scenario 1, where the attacker takes control of the car, the total number of cars affected will necessarily remain limited. The situation however looks very different if we consider scenarios 4, 5 and 6. As e.g. the recent ransomware attack against the UK hospital system showed, an almost unlimitedly large number of computers can be affected at the same time, using the same weakness in the attack against all of them[21]. While a traditional theft exploits the weakness of a specific car, in a specific location (e.g. parked out of sight from observers), an attack against the software system of autonomous vehicles could simultaneously target all the cars with that exploit.

[Rz 25] If every car hacking that compromises the software of an autonomous vehicle counts as theft of the vehicle – and above we gave some reason why this might be what the DoT proposes, then all these vehicles would be treated as stolen, rendering the insurance companies liable for the likely accidents on an epic scale (especially scenario 3 and 4, where software is deteriorated). Nor is it straightforward that they could get redress from the manufacturers. In many cases, these will be shielded by a «state of the art» defence, as the arms race between defensive and offensive programmers goes into its next iteration. Established ways of controlling exposure might not work under this setting either. In the aftermath of the Great Heck Rail Crash in 2001, where the mistake of a single driver caused over č22m in damages, car insurers in the UK began to limit the amount that they are liable for in the event of a claim for property damage against a legitimate policy. This is permitted under UK and EU law, though the EU Motor Insurance Directive requires that the minimum amount of cover in respect of damage to Third Party property is not less than €1,220,000.–, to be automatically adjusted in line with inflation every five years.

[Rz 26] However, while this allows insurers to cap the collective total amount due from a series of claims that arise from one single event, this still applies to individual policies. In our scenario, the massive attack against multiple cars, each covered by its own insurance contract, would mean a limit of č1m for *each individual* car that was involved.

[Rz 27] Given that the car manufacturers are best placed to counteract this risk by investing in cybersecurity embedded in the car's software system (unlike traditional theft, were the owner has a considerably larger role to play), insurance by the vehicle owner, rather than the manufacturer, is ill suited to enable insurers to reward risk minimising behaviour.

[Rz 28] So far, we discussed the harm to third parties when a hacked car is involved in an accident. But as our initial scenario shows, also the «driver» and passengers of the car are at risk. To determine if the legal response is adequate, one must also consider the position and insurance cover of the «driver» of a hacked vehicle as part of the legal equation. If a vehicle is maliciously manipulated while its owner is on board (and hence a «driver», especially if the car is not fully autonomous) and the vehicle is treated as stolen, then the «driver» is relegated to the position of a passenger of an uninsured driver. Passengers of non-insured drivers are protected by the insurance of the owner of the car or the Motor Insurance Bureau (MIB) but only if «they could not know that the driver was uninsured». If we follow the logic of the DoT proposal, the moment a vehicle was hacked (at least in scenarios 1 and 2 above), the thieves become the drivers, and

21 https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.

the owner (like any other passenger) are now driven by an uninsured driver. Moreover, as they probably know what is happening to them (especially in scenario 1, they would not be able to claim if they suffer injuries after the remotely controlled car crashes. Since the law should not encourage, under these conditions, to leave the moving vehicle by force, a different solution needs to be found.

[Rz 29] Finally, we also have to consider the situation where the car that has been hacked in not insured. From the liability perspective, if someone is injured by an uninsured stolen vehicle, then the claim is not against the owner of the vehicle but against a pool of money paid for by the insurance industry (MIB). This response and compensation is not equivalent to being hit by an insured driver.

[Rz 30] With the onset of autonomous vehicles, is society ready to accept this? Will the current fiscal-pot be adequately supported given that the liability trend will move from insured to uninsured agents?

7. The Unknown

[Rz 31] Legal mechanisms and propositions have great difficulty dealing with the unknown, which is why legislation is often broad and general. This ensures a degree of future-proofing to be built into the structure of the system while affording scope and interpretation further downstream in the process e.g. compliance controls, governance processes, standards, protocols etc.

[Rz 32] The DoT paper argues for an analogous treatment of hacking into a car with criminal manipulation undertaken in the physical world. In many ways, this is a sound analogy. It ignores however the special nature of cyberspace, where a single attack can have an almost unlimited number of targets, and where accountability and traceability is not a given. The report incorrectly identifies something it regards as a «known», when in most cases, this should be treated as an «unknown»:

> «*If an accident occurred as a result of an automated vehicle being hacked then we think it should be treated, for insurance purposes, in the same way as an accident caused by a stolen vehicle. This would mean that the insurer of the vehicle would have to compensate a collision victim, which could include the not at fault driver for damage caused by hacking but, where the hacker could be traced, the insurer could recover the damages from the hacker.*»[22]

[Rz 33] The pertinent point takes the form «where the hacker could be traced», with no regard to the vanishingly small likelihood of this being possible in most cases.

8. Traceability

[Rz 34] Traceability helps ensure accountability which in turn allows liability to be assigned to an offending party. Legally, assigning liability to either an insuring agency or the manufacturer can lead to scenarios that raise complications. Importantly, technical traceability is also a major consideration when determining whether malicious activity has taken place, raising further problems complicating the legal position.

22 DoT, Pathway to Driverless Cars 2016 (note 2), p. 21.

[Rz 35] Traceability can be divided into two categories:

1. Traceability of the hacker
2. Traceability of the manipulation

[Rz 36] Traceability of the hacker is not always easy[23] and existing tools make it very difficult, even for law enforcement officials.

[Rz 37] Tracing manipulation is an issue, not only when taken together with the scenarios presented previously but also when underlying algorithms are targeted. An attack that aims to control a car will have to follow a predictable pattern, and as a result leave identifiable digital traces as evidence. It seems less clear if this will also be the case for attacks that target the machine learning (ML) algorithms (an integral aspect of driverless cars[24]) not to achieve a specific goal, but simply to distrupt, distort and degrade the car's functions. This will require to separate malicious modification from «normal» behaviour, which may include intrinsic «mistakes»[25].

[Rz 38] This is further complicated by the opaque nature of the algorithms in-play, imposed upon us by the secretive nature of software development and the manufacturers testing procedures[26].

9. Conclusion

[Rz 39] The UK's proposal to support the emergent technology of driverless cars[27] and inform industry sectors on how to proceed and establishing a code of practice[28], is by and large a pragmatic approach, which, following in the footsteps of the US, aims at ensuring that the UK environment is a supporter of innovation and that evolving regulatory and legal mechanisms do not hinder progress.

[Rz 40] As stated in the DoT paper:

> «*We want to take a pragmatic and proportionate approach, with a rolling programme of regulatory reform.*»[29]

[Rz 41] The take away from this essay is that, by adopting a «rolling programme», new legal questions will be raised that aren't covered by the currently suggested approach relating to 3rd party hacking, liability, cost implications and identifying negligence. These areas aren't explored in the codes of practice and practical logistic elements need to be considered should tampering occur.

---

23 Alan Woodward, Viewpoint: How hackers are caught out by law enforcers, BBC News, 12 March 2012, available at: http://www.bbc.co.uk/news/technology-17302656.

24 Harry Armstrong, Machines that learn in the wild – Machine learning capabilities, limitations and implications, Nesta, July 2015, available at: https://www.nesta.org.uk/sites/default/files/machines_that_learn_in_the_wild.pdf.

25 Lisa Shay / Woodrow Hartzog / John Nelson / Gregory Conti, Do Robots Dream of Electric Laws? An Experiment in the Law as Algorithm, in: Ryan Calo / A. Michael Froomkin / Ian Kerr (Eds.), Robot Law, Edward Elgar Publishing, Gloucester 2013, pp. 274–305.

26 Andrew J. Hawkins, Uber dismissed warnings about its illegal self-driving test for months, emails show, The Verge, 27 February 2017, available at: https://www.theverge.com/2017/2/27/14698902/uber-self-driving-san-francisco-dmv-email-levandowski.

27 DoT, Pathway to Driverless Cars 2016 (note 2).

28 DoT, The Pathway to Driverless Cars: A code of practice for testing, 2015, available at: https://www.vicroads.vic.gov.au/~/media/files/documents/safety-and-road-rules/pathwaydriverlesscars.pdf?la=en.

29 DoT, Pathway to Driverless Cars 2016 (note 2), p. 8.

[Rz 42] As recent issues effecting the Internet of Things (IoT)[30] show, embedded systems are now a focus for hackers, and automobiles represent a very dangerous target which legal systems are struggling to cope with[31].

[Rz 43] As always, when confronted with technological change, two contradictory tendencies come into play: On the one hand, the apparent novelty of the technology often leads to demands for law reform. The problematic scenarios look different from the past, and that alone is seen as reason enough to update the legal provisions. This tendency is countermanded by our ability to recognise familiar patterns even in new surroundings. This, combined with the inherent slowness of the legislative process, pushes us to draw analogies between new problems and those of the past. It seems always easier to keep a tried and tested system in place than experiment with an entirely new approach. In the proposal of the DoT, this latter tendency by and large wins out. In UK Law it has always has been the duty of the car holder to ensure adequate insurance cover, and a part of this legally prescribed minimal cover also extends to accidents that occur when the car was stolen. For certain types of hacking attacks, this seems to provide an adequate solution, where past experience indicates that an overall small additional risk for the insurance companies provides substantial social benefits. These benefits are particularly pertinent when an as yet untried technology reaches the market and the public needs reassurance. However, as we have seen, this approach lumps together a range of rather disparate scenarios, and for some at least, the analogy to a traditional vehicle theft seem pernicious. There are some new forms of attacks against automated cars conceivable that have no equivalent under the old technology, and may require us to think about entirely new ways on how to allocate and collectivise the risk, if we want the technology to succeed.

Jonathan Sinclair holds a BEng (Hons) in Software Engineering, an MSc in Informatics and is half way through completion of his LLM in Information Technology Law, in addition to these academic qualifications he's a highly qualified IT security professional holding certifications from established bodies such as: (ISC)2, EC-Council, PECB, he's also a seasoned speaker having been invited to speak at Universities, IT security and AI conferences .

Burkhard Schafer, Professor of Computational Legal Theory, The University of Edinburgh, SCRIPT Centre for IT and IP law Old College, Edinburgh, EH8 9YL, UK. B.schafer@ed.ac.uk; http://www.law.ed.ac.uk/people/burkhardschafer.

30 Ben Herzberg / Dima Bekerman / Igal Zeifman, Breaking Down Mirai: An IoT DDoS Botnet Analysis, Imperva Incapsula, 26 October 2016, available at: https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html

31 Susan W. Brenner, Cybercrime and the Law: Challenges, Issues and Outcomes, Northeastern University Press, USA 2012.