Future Abuses of Driverless Technologies and Counter Measures

Alex Glassbrook[1], barrister and author of "The Law of Driverless Cars: An Introduction"[2], Temple Garden Chambers (London and the Hague)[3]

As technology innovates and expands, so do the opportunities for abuse. Alex Glassbrook considers the future vulnerabilities of driverless technologies to abusive and criminal behaviour. He reflects upon the lessons of defending fraudulent motor accident claims in the UK, and describes how the legal system responded to such claims. He examines how driverless technology might introduce new abuses, and how the law might respond effectively.

Introduction

Since 2011, with the first reported external hack of a car's internal systems[4], the vulnerabilities of modern cars to outside interference have been clear. With further advances towards fully driverless technology – and particularly the greater connectivity of vehicles to various devices and the internet - the opportunities for attack have increased.

[1] http://tgchambers.com/member-profile/alex-glassbrook/ . The opinions in this paper are those of the writer and not necessarily those of Temple Garden Chambers. This paper should not be relied upon as legal advice.
[2] Law Brief Publishing, February 2017: https://www.amazon.co.uk/Law-Driverless-Cars-Introduction/dp/1911035282
[3] http://tgchambers.com
[4] See page 5 of the report, "Remote Exploitation of an Unaltered Passenger Vehicle", 10 August 2015, by Dr Charlie Miller & Chris Valasek, at http://illmatics.com/Remote%20Car%20Hacking.pdf. Miller & Valasek reportedly controlled the car at greater speeds in 2016, though by a computer plugged in to the car, not remotely: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

In 2015, Dr Charlie Miller and Chris Valasek reported that they had been able to attack the driver assistance, WiFi and radio systems of a conventional vehicle (a Jeep Cherokee) remotely and to take remote control of its steering and braking and of the volume of the radio[5].

In September 2016, YouTube footage was released showing the controls of a vehicle with more advanced driver assistance systems (a Tesla), again being operated remotely by someone other than the driver. The footage showed the vehicle braking sharply and its wing mirrors folding inwards, apparently without those commands being given by the driver. The film claimed to show the Tesla being operated from several kilometres away, by employees of a security firm playing the part of a hostile third party[6].

The road vehicle industry – both manufacturers and many security firms (some of whom had demonstrated the vulnerabilities) – has responded. Faults have been patched. Several actors – including Intel and Uber– have sought the sharing of vehicle information, with the aim of increasing the security of vehicles "organically" by design, across the industry[7]. And in February 2017 the British government was among the sponsors of a competition, the purpose of which was to identify defensive cyber talent, in which the task was to "ethically hack" a fictional automotive company[8].

So traffic cybercrime is a challenge, both in terms of cybersecurity and as a direct threat to public safety on the roads. Equally challenging, though, is the need to retain the traveller's rights to privacy and confidentiality in an increasingly connected and security-conscious transport network.

I am a barrister in practice in the United Kingdom. Over the course of 21 years, I have appeared and advised in cases involving motor vehicles in many different contexts: in criminal and civil courts, in coroners' inquests into deaths in driving incidents and in litigation relating to damages for injury and for financial losses.

Those cases have variously involved disputes as to criminal and civil responsibility, the extent of recoverable damages, questions of statutory regulation, of public safety issues related to training and equipment, insurance law and, increasingly, the unravelling of apparent "accidents", which investigations indicate have been staged deliberately as part of criminal conspiracies to defraud third party motor insurers through false claims for compensation.

[5] Ibid, article at https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[6] https://www.youtube.com/watch?v=c1XyhReNcHY
[7] https://fastr.org/about-us/what-is-fastr-a-manifesto/
[8] https://cybersecuritychallenge.org.uk/news-events/hack-car-cyber-security-career-awaits

Fraudulent compensation claims pursued through the courts represent the chief financial abuse of the UK's system of compulsory third party motor insurance. These claims range from the small-scale fraud – the instant and opportunistic pretence of injury in an otherwise genuine collision - to the manufacture of false claims on an industrial scale.

Those larger frauds are supported by a criminal infrastructure supplying both the tools of the fraud (including vehicles and false claimants) and the means to secure and launder its proceeds (sometimes including fake accident management companies).

Motor insurance fraud has been among the most prominent traffic crimes in the UK for years. It has become a very profitable crime, estimated to cost the British insurance industry over £1 billion annually[9]. Among its effects is the criminalisation of drivers persuaded to take part on the false promise that insurance fraud is a victimless crime. There have been reports of its proceeds being channelled into other, highly serious criminal activities[10].

Driverless technology will be a target area for criminals. The categories of potential frauds and abuses of automotive technology are not closed. As the technology innovates, so will the opportunities for abuse.

While the methods and technology will become ever more sophisticated on both sides of the battle, the aim of the fraudster will remain, conversely, straightforward: to obtain the maximum profit, by the least costly means. "Least costly" implies methods that are resilient to detection, so the tools used to expose fraud need to be robust.

The legal profession in the UK has played a key role in the fight against motor insurance fraud. My chambers (Temple Garden Chambers[11]) has been in the vanguard and is the only set of barristers' chambers in the UK recommended for its excellence in Motor Insurance Fraud litigation by the legal directory Chambers & Partners. I am one of the barristers individually recommended as a leading practitioner in the field. My book "The Law of Driverless Cars: An Introduction" was published in February 2017.

In this talk I shall focus upon financially-motivated crime. But some of the following points would also apply in relation to differently-motivated crimes.

[9] https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/ifed/Pages/Types-of-insurance-fraud.aspx
[10] http://www.insurancefraud.org/IFNS-detail.htm?key=19506
[11] http://tgchambers.com

For reasons that I shall describe, counter-fraud in transport has been a fight more often fought in the civil courts than it has been prosecuted in the criminal courts. That is a feature which, in my view, needs to be addressed.

Even with increasingly impressive technologies – including, for example, sophisticated telematics providing speed and other vehicle data – a trial of issues in a road traffic case remains a complicated task, requiring precise analysis and presentation. And the process of unravelling and understanding evidence depends, still, not only upon information recorded electronically (such as images taken on mobile devices), but also to a very great extent upon the evidence of human eye witnesses.

That is unlikely to change. As technology expands the capabilities of automated vehicles, towards fully "driverless" capabilities, so shall the opportunities for fraud and the need for evidence from all sources – machine and human – increase. As the "internet of things" spreads across public and private transport, the justice system will need to adapt to the task of adjudicating cases involving the new technologies.

And in future, as the quantity of information processed by road vehicles increases, the rights of road travellers to privacy and confidentiality might become as familiar a topic as the presumption of innocence in the face of a criminal charge.

(1) Future vulnerabilities of driverless technologies to abusive and criminal behaviour

I shall not deal with offences against data protection laws, which shall be dealt with by other speakers. Both mass scale attacks (eg. denial of service, ransomware) and individual cyber attacks (eg. a targeted ransomware attack on a moving vehicle) are undoubtedly among the dangers being considered by the transport and security industries.

In addition to those cyber attacks, there are also likely to be attempts at very "low tech" attacks, eg. fraudsters posing as victims of collisions with automated vehicles, either as:

- drivers of non-automated vehicles inducing a collision by pulling out or suddenly braking in front of an automated vehicle (what is currently known as a "slam-on" type of induced accident, in which the fraudster driver is also typically accompanied by several fraudster passengers, who all bring claims),

  or as:
- fraudster pedestrians, "stepping out" in front of a driverless vehicle.

Those are both risky frauds: risky in terms of their vulnerability to detection (especially by telematics and cameras on the vehicles themselves) and in terms of the risk of actual injury to the

fraudster. But both of those risks have long existed in motor insurance frauds (accompanied by heavy prison sentences, if the fraudster is detected and prosecuted) and neither risk has proven to be a complete deterrent to date.

Indeed, improvements in vehicle safety technology (especially in sensors, speed limitation and vehicle body design) might increase the prevalence of attempted frauds, by reducing the risk of injury to the fraudster. The emerging liability theory of driverless cars – that either manufacturer or insurer will bear liability and therefore the compensation bill for any injurious fault in an accident involving a driverless car – is also a potential enticement to fraudsters, as it tends to increase the perceived chance of compensation.

The practised fraudster will be adept at contriving a collision just at the moment when injury is plausible but, simultaneously, when the risk of actual injury is at its lowest. This has been the case in motor insurance frauds in the UK, in which a skilled criminal driver is sometimes in charge of the target car at the point of collision, neatly steering and braking the car into collision precisely at the desired moment, and then switching places with the claimant driver in the moments of surprise to the innocent defendant after the collision.

In that scenario the complicit claimant driver, who later brings the claim against the insurer of the innocent driver, has usually been selected on the basis of his or her clean insurance record. This is a good example of risk assessment and risk avoidance by well-prepared criminals.

It is possible to detect, reveal and demonstrate such frauds to the courts by careful investigation of the circumstances of a claim, of networks of relationships and by precise representation at trial. Legal principles such as that set out in the 2005 judgment of the House of Lords in *O'Brien v Chief Constable of South Wales Police*[12] allow a robust, forensic defence of a civil claim reasonably suspected to be fraudulent (that is the principle that circumstantial evidence of a party's similar misbehaviour requires no test more demanding than relevance to the issues to be admissible evidence in a civil claim).

And, after a finding of fraud in a civil trial, the laws of false evidence (perjury) and court procedural rules governing committal for contempt of court[13] allow the transformation of a sufficiently serious case from a purely private, financial claim for compensation, into a public and criminal law

[12] [2005] 2 AC 534

[13] Civil Procedure Rules 1998 ("CPR") Part 32.14 (false statements: "Proceedings for contempt of court may be brought against a person if he makes, or causes to be made, a false statement in a document verified by a statement of truth without an honest belief in its truth") and Part 81 (applications and proceedings in relation to contempt of court).

matter, and thereby to allow perjury to be tried and punished criminally, to the criminal standard of proof (beyond a reasonable doubt), where appropriate.

Where such criminal behaviour is proven to have occurred in a civil claim for damages, the sentences are appropriately heavy, as was made clear by Lord Justice Moses in the 2011 judgment in *South Wales Fire and Rescue v Smith*[14]:

> "Those who make such false claims if caught should expect to go to prison. There is no other way to underline the gravity of the conduct. There is no other way to deter those who may be tempted to make such claims, and there is no other way to improve the administration of justice."

So the tools of detection and trial exist to combat abuse, when it occurs. What are the future risks of abuse? Without meaning to suggest the means of future crime, the foreseeable risks now include the following:

- the staging of fake accidents, as described above, in an attempt to defraud manufacturers or insurers of compensation (faked accidents, whether by the occupants of other vehicles or pedestrians)
- hacking a moving vehicle (as indicated by Miller, Valasek and others) covertly in service of a contrived accident (faked accident, above)
- a ransomware attack on a moving vehicle, overtly in an attempt to obtain swift payment for return of control of the vehicle (individual ransom attacks)
- threatening such ransomware attacks on more than one moving vehicle simultaneously (a mass ransom attack, aimed for example at the operating company or a vehicle software provider)
- attacking or threatening to attack the controls of moving vehicles or their systems, maliciously rather than for financial gain (criminal damage)
- Thefts of valuable data that is either stored in or passes through the systems of the vehicle (data theft).

The categories of potential abuses are sadly not closed. Innovation carries the risk of multiplying the vulnerabilities to abuse (eg. by increasing the number of "attack surfaces" on a vehicle).

And, as you will have noticed, the last four examples require no use of the court system by the criminals, as part of the fraud. Those would be matters purely for the criminal courts, after detection by the police. That is a topic to which I shall return.

[14] [2011] EWHC 1749 (Admin)

(2) The lessons of defending fraudulent motor accident claims in the UK

As an advocate appearing, over many years, for one or other side in the trials of many cases of suspected motor fraud (though chiefly on the side of the insurer asserting fraud), I observed the following trends.

The frauds grew more sophisticated – and learnt from the legal process. That continues to happen: fraudsters learn about the legal process - and draw conclusions as to how better to present their cases.

Political attempts to legislate to remove the main source of such claims (soft tissue whiplash injury compensation claims) have so far been unsuccessful – not only because such attempts would outlaw a large proportion of entirely legitimate claims, but also because the fraudsters would adapt and look elsewhere.

The tools of counter fraud litigation have changed. In particular, new technology has been put to the task of countering fraud. That is true especially of:

- On–vehicle cameras, eg. on buses
- Telematics on vehicles (initially on emergency services, rental and commercial vehicles, to record mileage, driving times, location and data in the event of an accident, but also increasingly encouraged by motor insurers of private drivers. Telematics also include accelerometers, showing changes in the motion of a vehicle, eg. heavy breaking, accident reporting systems and – as on buses - internal and external cameras)
- Location data from routinely-used devices such as dashboard or helmet-mounted digital cameras, cameras on smartphones, Satellite Navigation systems, whose images, data and metadata have become useful tools from which to deduce the circumstances of a collision.

As well as the use of expert evidence at trial, especially:

- Expert forensic engineering evidence, especially to detect signs inconsistent with the alleged accident, eg. height differences between the damage marks on allegedly colliding vehicles; damage inconsistent with alleged impact speed; marks on tyres inconsistent with a vehicle being in motion.
- Expert evidence as to interpretation of data (such as that shown on insurance records or telematics equipment)

- Professional fraud investigation into circumstantial evidence of fraud, including histories and relationships of people and vehicles – applying the principles in the *O'Brien v South Wales Police* judgment, above.

  And by publicly accessible, location information online, where authoritative or agreed between the parties (especially maps and satellite images)

  And, overall, by:

- Fighting the cases in court.

However, the frauds have also evolved. I can recall one trial in which I had the strong impression that the large group in the public gallery, evidently all supporters of the opposing side, were listening to my cross examination with a close professional interest. Methods have become more sophisticated.

(3) How the British legal system responded to fraudulent motor claims

The courts took some time to realise that motor insurance fraud was a real phenomenon and not merely the product of a suspicious corporate imagination on the part of motor insurers.

As more cases came before the courts, trends began to emerge – including the use of particular postal addresses by large numbers of Claimants for road traffic injury, in alleged accidents occurring over certain periods of time and in locations and accidents very similar to each other. Some cases showed evidence of repeated use of particular mobile telephone numbers, postal addresses and aliases.

The circumstances in such cases suggested dishonesty as the greater likelihood than pure coincidence. The evidence was often very strongly suggestive of fraud.

As the courts became more aware of the phenomenon, they responded. In particular, the law was altered in the following ways:

- To allow a defendant to a civil claim for damages to defend a claim not only on the basis that the claim was fraudulent but also (in the event that the assertion of fraud was not accepted) on the basis that the claimant had failed to prove his claim on the balance of

probabilities. That was the effect of the judgment of the Court of Appeal in the case of *Francis v Wells*[15].

- To allow a dishonest claim to be struck out as an abuse of the process of the court (exceptionally, even after trial, if it was then proportionate to do so). That was achieved by judgment of the Supreme Court (in *Fairclough v Summers*[16]).
- By the exception written into the "Jackson" system of legal costs introduced in 2013 (named after its designer, Lord Justice Jackson), whereby a claimant whose claim was shown to be "fundamentally dishonest" would be deprived of the protection otherwise available to him (protecting him from any costs order being enforced beyond the level of any damages recovered). A fundamentally dishonest claimant would be exposed to the full extent of costs orders against him, which would in that case typically amount to an enforceable order that he pay the entire costs bill of both sides.

So awareness of motor insurance fraud and the courts' capacity to deal with it increased (including by use of its procedural powers to commit for contempt of court).

But motor insurance fraud was dealt with essentially as an aspect of civil litigation. That was natural, because the fraud took the form of a civil claim for damages, so the fraud case arose as a civil defence. As a matter of law and professional conduct, such defence can be pursued only where the evidence, properly considered by counsel instructed to consider fraud, is sufficiently strong to support that serious allegation[17].

But, as the list of potential frauds and abuses in the driverless world shows, many of the foreseeable attacks will not arise in this way. Those abuses (including ransomware attacks) will not require a civil claim. Those will be unequivocally criminal activities.

That will be a change. As I have described, the defence of fraudulent RTA claims – the major abuse - has taken place mainly (if not exclusively[18]) in the civil courts, by way of defences to civil claims for damages. As I shall describe, that has shaped the infrastructure of road traffic fraud defence in the UK. That infrastructure will, in my view, need to change.

---

[15] [2007] EWCA Civ 1350
[16] [2012] UKSC 26, [2012] 1 WLR 2004
[17] *Medcalf v Mardell* [2003] 1 AC 120 (HL)
[18] See eg. *R v Samra & El Habbal* [2014] EWCA Crim 2748. But RTA fraud defence has stemmed mainly from the defence of civil claims.

(4) How the law might respond effectively to new abuses

British criminal law already provides tools to deal with abuses such as ransomware attacks.

In particular, section 3ZA of the Computer Misuse Act 1990 was introduced by amendment in May 2015, with mass attacks (including terrorist attacks) on "critical national infrastructure"[19] in mind. One leading commentator has expressed the opinion that the Section merely duplicates existing powers and that "It seems unlikely that s.3ZA will be used often, if at all"[20].

But the terms of Section 3ZA (which carries sentences of imprisonment of up to 14 years or for life, if there is risk of serious damage to human welfare[21]) would appear to fit the prosecution of a ransomware attack on a moving driverless or driver-assisted vehicle. These (with my added italics) are the relevant parts of the Section:

> "**3ZAUnauthorised acts causing, or creating risk of, serious damage**
>
> (1) A person is guilty of an offence if—
>
> (a) the person does any unauthorised act in relation to a computer;
>
> (b) at the time of doing the act the person knows that it is unauthorised;
>
> (c) *the act causes, or creates a significant risk of, serious damage of a material kind*; and
>
> (d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.
>
> (2) Damage is of a "material kind" for the purposes of this section if it is—
>
> (a) *damage to human welfare in any place*;
>
> (b) damage to the environment of any place;
>
> (c) damage to the economy of any country; or
>
> (d) damage to the national security of any country.
>
> (3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes—
>
> (a) *loss to human life*;
>
> (b) *human illness or injury*;
>
> (c) disruption of a supply of money, food, water, energy or fuel;

---

[19] Crown Prosecution Service guidance at http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/
[20] Professor Andrew Murray, "Information Technology Law: The Law and Society" (3rd edition, Oxford University Press, 2016) at page 383.
[21] CPS guidance, footnote above.

(d) disruption of a system of communication;

(e) *disruption of facilities for transport*; or

(f) disruption of services relating to health.

(4) It is immaterial for the purposes of subsection (2) whether or not an act causing damage—

(a) does so directly;

(b) is the only or main cause of the damage.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.

(6) A person guilty of an offence under this section is (unless subsection (7) applies) liable, on conviction on indictment, to imprisonment for a term not exceeding 14 years, or to a fine, or to both.

(7) Where an offence under this section is committed as a result of an act causing or creating a significant risk of—

(a) serious damage to human welfare of the kind mentioned in subsection (3)(a) or (3)(b), or

(b) serious damage to national security,

a person guilty of the offence is liable, on conviction on indictment, to imprisonment for life, or to a fine, or to both."

As to the ability of victims, insurers and manufacturers to recover damages against hackers, there is debate as to the availability of a remedy in the tort of trespass against property, on the ground that there is some doubt as to whether the mere "accessing [of] data rather than altering it ought to amount to trespass". The question of whether or not data has been altered might therefore arise, though that might be mainly a question of fact.

A leading practitioner's work also notes that the defendant hacker would then need to invoke the defence that his act had "not gone beyond generally acceptable standards of conduct"[22], which

[22] Clerk & Lindsell on Torts (21st edition, 2014, Sweet & Maxwell) at 17-136.

would seem unlikely to succeed as a defence in the case of hacking of a vehicle, with the associated dangers to human safety.

So hacking of vehicles seems capable both of prosecution and of constituting an actionable civil wrong (of trespass against property) in tort law.

But the greater part of the future threat to driverless and driver-assisted cars appears to be in criminal law territory. So there needs to be a strong cyber-security infrastructure in policing.

The British government's current, five-year cyber security strategy seems to recognise that need:

> "Law enforcement agencies will collaborate closely with industry and the National Cyber Security Centre to provide dynamic criminal threat intelligence with which industry can better defend itself, and to promote protective security advice and standards".[23]

The aspiration of interagency co-operation is easily stated. But, given the clear likelihood of vehicle cybercrime, traffic police will need much better resources in order to have an effective counter-fraud capability. In particular, traffic police will need to be equipped to detect the possibility of cybercrime in road traffic accidents. That (as Miller and Vasalek have demonstrated) is a danger not restricted to fully-automated vehicles, though it is likely to increase markedly as that technology advances.

That detective capacity will require a change in British police investigative policy relating to road traffic accidents. It might imply attending the scene of every accident. Now, police policy tends against investigating allegations of suspicious behaviour that might indicate motor insurance fraud.

To some extent, the insurance industry has been a victim of its own successes in contesting fraudulent claims in the civil courts. While there have been some notable successes in prosecuting road transport fraudsters, the insurance industry has tended, even there, to take the leading role (as, for example, in the foundation of the Insurance Fraud Bureau[24], to support police RTA fraud investigations).

The phenomenon of cautious police involvement is well-known to those dealing with such cases. The following policy of one British police force illustrates the general point:

---

[23] The British Government's "Cyber Security Strategy 2016-2021", page 33, para.5.0.2, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[24] https://www.insurancefraudbureau.org/about-us/supporting-law-enforcement/

"Over 80% of Derbyshire Police non-injury collisions investigations do not result in further police action being taken against the parties involved once initial details have been obtained. It is for that reason that reports of non-injury collisions should be resolved at the first point of contact (FPOC) if possible without the allocation of a police officer. Non-injury collisions should be resolved at the FPOC where:

- Details have already been exchanged and an allegation, even if proven, is unlikely to lead to a criminal justice outcome for the offending driver such as a driver improvement course or court prosecution. In these cases, it is for the complainant's insurers to establish who was at fault. Police officers should not take statements from witnesses unless a prosecution is being considered. Examples of cases unlikely to be in the public interest to prosecute and lead to a criminal justice outcome include:
    - Low speed collisions in retail car parks, where there has been minimal error in judgement and no tangible risk of injury.
    - Low speed collisions when parking on a road where no pedestrian, cyclist, motor-cyclist or other vulnerable road user was put at risk by a minor lapse of driver/rider judgement.
    - A low speed, rear-end collision on a road where there has been a minimal error in maintaining the correct braking distance."[25]

However, all three of those scenarios arise frequently as the basis for suspected fraudulent claims for injury to the occupants of the vehicles, as (a) low speed impacts carry the least risk of actual injury to the perpetrator and (b) it is often said that the symptoms of injury do not manifest immediately, so might not be mentioned to a police officer at the scene, even though an injury claim will swiftly follow. An officer without specialist training in existing road traffic frauds might either not recognise the possibility of an attempted fraud, or recognise it but be discouraged by his official guidance (as above, requiring a likely criminal fraud conviction) from taking the suspicion any further.

The reason for the police policy of referring the complaint to the complainant's insurers (who are then left to defend the claim) appears to be resources, and the perception that insurance companies have the greater capacity than the police to investigate fraud and to seek quasi-criminal punishments (eg. for giving false evidence in a subsequent claim).

[25] http://www.derbyshire.police.uk/documents/about-us/freedom-of-information/policies/roadtrafficcollisionsreportsprocedure.pdf

Advances in vehicle technology – particularly driverless technology and the increasing connectivity of vehicles – will provide new tools for fraudsters. In particular, the possibility of hacking a vehicle's controls to induce a collision arises.

So the UK government's cybercrime strategy will need a traffic aspect. It will demand more operational tools than traffic police are currently given, eg. training in cybercrime for police accident investigators and the capacity for traffic officers to recognise and seize evidence of possible cybercrime, at the scene of an RTA. Those tasks would demand investment, to fund the training, equipment and salary for specialist police officers. It is difficult to see how the introduction of artificially intelligent vehicles onto the roads, and the clear risk of traffic cybercrime, would not require those measures as a matter of public safety.

More officer training – including training as to the application of cybercrime offences to vehicle (under the Computer Misuse Act 1990) - should be considered. The vehicle industry might be involved in that training – perhaps as part of the "organic" approach to cyber security that Uber, Intel and others have suggested. In this, there is an echo of the findings of the Rand Corporation's survey of law enforcement officers in the United States, who found that:

> "Some of the highest-ranked needs were not futuristic pieces of hardware at all, but information and training to help police make more effective use of the technology they have."[26]

The Courts

The International Bar Association's recent report on the effect of AI and robotics upon the employment market[27] predicts that many human "reasoning" jobs will be carried out by robots. We have seen the beginning of that in risk assessment for insurance underwriting. The counter-fraud writer David Morrow has suggested that fraud detection might itself become automated:

> "AlphaGo [*which, as many in the audience will know, is a computer playing a human grandmaster in a sophisticated chess-like game*] won by consistently taking the right decisions. This leads me to believe that technology will be able to deliver a fast, accurate, autonomous fraud management capability as well. I'd sell my grandmother for an 'AlphaFraud' intelligent agent application which combines

[26] Rand Corporation article, 7 January 2016: "How will technology change criminal justice?", at https://www.rand.org/blog/rand-review/2016/01/how-will-technology-change-criminal-justice.html. Rand Corporation report August 2015, "Using Future Internet Technologies to Strengthen Criminal Justice" at https://www.rand.org/pubs/research_reports/RR928.html

[27] https://www.ibanet.org/Article/NewDetail.aspx?ArticleUid=012a3473-007f-4519-827c-7da56d7e3509

> advanced search techniques with neural networking, allowing it to think creatively and take advantage of huge amounts of data about previous frauds and current behaviours."[28]

But that does not allow for the process of *proving* a fraud, by a fair hearing in a court of law, unless the courts also become fully automated. That seems very unlikely. The burden of proving criminality must remain with a prosecutor and – absent a truly dystopian solution – the adjudication of whether or not a person is subject to punishments for criminality should always be a human rather than a mechanical process.

If so, then the disadvantage of a fully-automated fraud investigator would be that its artificially intelligent reasoning must be translated back into terms that human intelligence can grasp, dissect and examine in the courtroom. That process might reveal important gaps in the artificial reasoning process – see by analogy the development over time of safeguards concerning the use of DNA evidence in criminal cases[29]. These points sound trite after the event, but the excitement of an emerging technology can lead to over-optimism as to its capacity.

Just as the police will require greater capacity, so will the courts. A large proportion of the work of the County Courts (the first level of civil courts in the UK) is attributable to road traffic accidents. The police policy of diverting questions of fraud from the criminal to the civil courts (above) is in part responsible for that.

The better course might be for future transport crimes to revert to the criminal process and not be left to motor insurers to litigate in the civil courts. The point is especially forceful where traffic cybercrimes are concerned. A cyber attack on any moving vehicle (interfering with its systems while it is in motion, whether to induce an accident or otherwise) would be a very serious attack upon public safety at large.

The possibility of cybercrime should not be left uninvestigated and evidence missed at the scene, by police policy remaining in its current state. It should not be left to insurance companies to detect, particularly because the civil courts lack the criminal law tools (eg. the Computer Misuse Act 1990) properly to deal with such an offence.

The legal questions coming before the courts will alter. It will be the job of lawyers to assist the courts in that change.

---

[28] "AI is the Future of Fraud Management" by David Morrow, 23 May 2016, at https://commsrisk.com/ai-is-the-future-of-fraud-management/

[29] See pages 15 to 18 of the British Forensic Science Service's booklet, "Guide to DNA for Lawyers and Investigating Officers" (FSS, 2nd edition, 2004) at https://www.cps.gov.uk/legal/assets/uploads/files/lawyers%27%20DNA%20guide%20KSWilliams%20190208%20(i).pdf.

But the courts will also need to be better equipped. On a routine level, the high dependence of courts upon paper must come to an end. Counter fraud cases already turn to a great extent upon originally digital documents - from images taken on smartphones to insurance company records. Those documents are often far more easily navigated and understood on a screen than on paper, because they are digital in their original form.

And digital documents are more easily transmitted digitally, between parties and the court. Reliance upon multiple paper copies of documents extends the time required to prepare a case and can delay trials. American law enforcement officers interviewed by the Rand Corporation for its August 2015 report, "Using Future Internet Technologies to Strengthen Criminal Justice", noted the problem of delay in criminal courts in the United States, and suggested the further use of technology to co-ordinate the timing of hearings more effectively. Those are not new problems.

Again, properly equipping the courts in terms of judicial training and equipment will require significant investment. But, again, the wider aim is public protection, in which the proper administration of justice plays a crucial part.

Conclusion

The detection of abuses will require greater levels of training and expertise in policing as well as in the criminal and civil courts. This will require investment in court services (especially digital infrastructure) as well as a change in attitudes, eg. towards the use of paper as the main medium in court cases. But the evidence itself will come from a mixture of artificial and human sources. And its interpretation will have to remain a primarily human activity – at least until we can completely explain both our own cognitive processes and those of machines.

Alex Glassbrook
Temple Garden Chambers
1 Harcourt Buildings
Temple
London
EC4Y 9DA
ag@tgchambers.com