SOUTH AFRICAN REPORT

By

DALEEN MILLARD[1*]

And

SAMANTHA HUNEBERG[2*3*]

I. DRIVERLESS/AUTONOMOUS VEHICLES AND VESSELS

1 Are there any specific laws already adopted in your jurisdiction, or proposals for laws, relating to liability in tort for injuries inflicted by the use of such vehicles or vessels? If so, please provide a short explanation.

Comment: answers may include the liability of drivers, producers of vehicles and the suppliers of satellite technology.

A. DRONES

Yes, Part 101 of the South African Civil Aviation Authority Regulations contains extensive provisions on the use of drones. Part 101.4 deals with the certification of obtaining a RPAS operations certificate which states that: "(1) No person shall operate an RPAS in terms of this Part unless such person is the holder of – (a) in the case of commercial, corporate and non-profit operations, a valid ROC including the operations specifications attached thereto."[4] With regard to insurance it states that "[a]n ROC holder shall at all times be adequately insured for third party liability". It is thus clear that for all commercial operators of RPASs, third party liability insurance is compulsory. However, there is no such obligation on private use operators in South African law.

Prior to 2015, the flying of drones was entirely unregulated in South Africa, which therefore rendered the flying of these systems illegal. Initially, the South African Civil Aviation Authority (SACAA) responded to the major uptake in the use of drones by clamping down on such systems which were already in operation in the South African civil aviation airspace.[5] In 2014, SACAA issued a media statement in which it explained that the current civil aviation laws did not provide for the certification, registration or operation of drones in the South African civil aviation airspace.[6] SACAA also stated that anyone flying any type of drone in South Africa was doing so illegally.[7] In the

---

[1*] BIUR LLB LLM (UP) LLD (UJ) Vice Dean and Professor of Private law, University of Johannesburg.

[2**] BCom LAW LLB LLM (UJ) Assistant lecturer in Commercial Law, University of Johannesburg.

[3]

[4] Part 101.04.1.

[5] SACAA "Civil Aviation Authority to crackdown on illegal drone flying" (2 April 2014) http://bit.ly/2ndHXYp (accessed 11/11/16).

[6] SACAA "Statement on unmanned aircraft systems" (3 June 2014), available at http://bit.ly/2mypSat, accessed on 2016-11-11.

[7] See fn 2.

statement, SACAA mentioned that they were developing regulations to deal with the burning issue at hand and in doing so, safety, security and privacy were major concerns that had to be considered by the Authority.[8] However, SACAA had since collaborated with the drone industry and had formulated regulations to regulate this rapidly expanding industry.[9]

The current South African drone regulations came into effect on 1 July 2015 and are among the most stringent in the world.[10] These regulations state that anybody above the age of 18 will be allowed to purchase a drone – with or without a licence – but the regulations restrict the use of drones. It is generally accepted in modern times that as technology progresses, so too must a country's laws. The law cannot stagnate and must be developed in such a way so as to cater for technological advances. Drones have existed for at least two decades but their application was extremely limited due to the high costs of having these types of systems and therefore, they were not readily available to most people. However, there is currently an increased demand for drones and as a result additional regulation is required.

All drone usages are effectively regulated by legislation.[11] The newly adopted drone regulations, known as Part 101, apply to all drone usage including *private use* as well as *commercial use*.

Private use regulation is restricted and entails that the user of the drone has no commercial interest; the drone is operated on property owned by the operator (or on property that the operator has the necessary permission to fly on); and distance thresholds – 500m from the pilot and never higher than any obstacle within 300m from the pilot – of operation are maintained.[12] There is no obligation to have the Remotely Piloted Aircraft (RPA) approved and registered nor is there a licensing requirement. Part 101 provides with regard to private use of RPAs/UASs that "[p]rivate operations means the use of an RPA for an individual's personal and private purposes where there is no commercial outcome, interest or gain".

The significance for "private use" in insurance is quite clear. Although short-term insurance policies are primarily classified in accordance with the definitions contained in section 1 of the STIA (such as motor policies, engineering policies, and so forth)[13] there is a further distinction between products that are grouped together under so-called "personal lines" and those that resort under "commercial lines". The distinction between private and commercial insurance relates primarily to the kinds of insurance products that are sold and secondly, to the classification of the intermediaries who sell these products. It stands to reason that where legislation also distinguishes between private use and commercial use,

---

8 *Ibid.*
9 Part 107 of the South African Civil Aviation Authority.
10 As formulated by SACAA in Part 101 of the Regulations.
11 Part 101 of SACAA.
12 Part 101.01.2 of SACAA.
13 Millard *Modern insurance law in South Africa* (2013) 39.

the owner or operator of a drone should be careful to license the drone according to its primary use (commercial or private) first and secondly, to procure suitable insurance.

There is the perception that commercial insurance is more expensive than private insurance and that where a drone owner or operator who uses the drone for commercial purposes ensures it erroneously for private purposes, the insurance will be insufficient and subsequent risks will most likely not be covered. Insurers like Santam are offering insurance for both private and commercial use drones.

Commercial use: Where a drone is operated for anything other than private use, the drone must first be approved and registered by SACAA.[14] The operator of the system will also require a RPA pilot's licence.[15] Acquiring the licence requires medical certification, certification of radiotelephony, English proficiency, flight training, and passing both a theoretical examination and skills test.[16] The licence is valid for 24 months and applicants must be over 18 years old.[17] The licence holder will also have to undergo a revalidation check 90 days prior to the expiry of the licence in order to renew it.[18]

Part 101 states the following with regard to commercial use of a RPA:

> "No person shall act as a remote pilot, except when undergoing a skills test or receiving flight instruction, unless he or she is in possession of a valid remote pilot's licence (RPL) in the relevant category. Prior to making any application with SACAA, an applicant should obtain aviation training from an approved training organisation. An applicant should not be less than 18 years of age. Applicants must hold current medical assessments. Applicants must pass the RPL practical assessment. Applicants must also pass at least restricted Radiotelephony Examination. Applicants should achieve English Language Proficiency level 4 or higher."

Under the new regulations, RPA operators will also be required to maintain a pilot logbook detailing each flight. The registration and marking of RPAs are also dealt with in part 101. It states that "[n]o RPA shall be operated within the Republic, unless such RPA has been issued with a certificate of registration by the Director".[19] The SACAA also requires a letter of approval for the use of a Remotely Piloted Aircraft System (RPAS).[20] The section states that "no RPAS shall be operated within the Republic, unless such RPAS has been issued with a letter of approval by the Director".[21] The general regulations on the use of any drone – including for private use – also include the regulations pertaining to compulsory pre-flight preparations. In addition, they limit the operation to a

---

14 Part 101.02.4.
15 Part 101.03.1.
16 *Ibid.*
17 *Ibid.*
18 *Ibid.*
19 Part 101.02.4.
20 Part 101.02.1.
21 Part 101.02.1.

lateral distance of 50 metres from any structure or public road, require that the operator maintains at least a 10 per cent surplus fuel reserve, and that there should be a first-aid kit and a fire extinguisher within 300 metres of the take-off and landing point(s). Furthermore, considering traffic, drones must always give way to manned aircraft. SACAA may grant specific permissions for night operations and operations in the vicinity of people, property, structures and buildings, and public roads.[22]

B. AUTONOMOUS VEHICLES

There are no new laws or proposals for new laws. There is a distinction in South African law between damage caused to motor vehicles (material damage) and personal injuries (which includes death). Damage caused to motor vehicles are determined by the *actio legis Aquilia* which requires five elements, namely an act (which includes an omission), wrongfulness, fault, causation and damage.[23] There is an argument to be made that these principles are adequate to address damage caused by autonomous vehicles.

Personal injuries caused by the driving of a motor vehicle is regulated by the Road Accident Fund system. The Road Accident Fund Act[24] 56 of 1996 came into operation on the 1 May 1997 and the main purpose of this act was to replace the wrongdoer with a statutory fund (the Road Accident Fund). With a few exceptions, the RAF system was based on Aquilian liability and the funding came from a fuel levy imposed on petrol and diesel. The Road Accident Fund Amendment Act, 2005 came into operation on the 1 August 2008 and this amendment act had the purpose of capping compensation for pain and suffering. This implied that only victims who sustained serious injuries were entitled to a limited amount of money for pain and suffering. The MVA system indemnifies the driver or owner of a motor vehicle against liability incurred as the result of the loss or damaged wrongfully caused to another person in road accidents caused by motor vehicles. This system is evidently not one where private insurers have a role to play, save to market and sell top-up products.

The Road Accident Benefit Scheme (RABS) is a proposed replacement for the current Road Accident Fund (RAF), which is a state-supported insurance fund designed to provide compensation for those seriously injured in motor vehicle accidents on South African roads. The new system will not be fault-based and where there will be an increase in claims as a result, it is expected that this will be counter-balanced by capped compensation. The definition of "motor car" in the current RAF Act is as follows: "A "motor car" means a motor vehicle designed or adapted for the conveyance of not more than 10 persons, including the driver". This will include an autonomous vehicle, unless the statutory regime is changed to exclude autonomous vehicles from this definition, in which case autonomous

---

[22] Operators must consult with the SACAA prior to any of these flights.

[23] Neethling J and Potgieter JM *Neethling Potgieter Visser's Law of Delict* (2015) 4.

[24] 56 of 1996.

vehicles will have to be insured to cover material damage to the vehicle itself and personal injury or death caused to passengers.

2. Are there any specific laws already adopted in your jurisdiction, or proposals for laws, relating to compulsory insurance coverage for injuries inflicted by the use of such vehicles or vessels? If so, please provide a short explanation.
Comment: answers may relate to motor vehicle insurance and product liability insurance.

A. DRONES

For drones the answer is "yes". Part 101.4 deals with the certification of obtaining a RPAS operations certificate which states that: "(1) No person shall operate an RPAS in terms of this Part unless such person is the holder of – (a) in the case of commercial, corporate and non-profit operations, a valid ROC including the operations specifications attached thereto."[25] With regard to insurance it states that "[a]n ROC holder shall at all times be adequately insured for third party liability". Once again, only commercial operators of RPASs are compelled to take out third party liability. There is no obligation on private use owners currently.

Section 155 of the Civil Aviation Act requires owners of aircraft to have liability insurance. It is necessary to identify the three different types of risks or insurance, namely, damage to the drone itself, damage to third parties and their property and surface damage (for which strict liability is imposed). Section 8(5) of the CAA states the following: "A registered owner or operator[26] of an aircraft must have insurance as prescribed for any damage or loss that is caused by an aircraft to any person or property on land or water." This section would therefore be applicable to UAS/RPASs as well,[27] due to the fact that it refers to "aircraft" and from the definition of the Act, it can be inferred that UASs fall under this definition.[28]

As far as *liability insurance* is concerned (for strict liability in case of surface damage) and liability to third parties, insurers are not limited to a statutory minimum. Rather, they consider the nature of the

---

25 Part 101.04.1.

26 "Operator" means a person or artificial entity, holding a valid licence and operating certificate or equivalent thereof authorising such person to conduct scheduled, non-scheduled or general air services, and airline, air carrier, air service operator or commercial air transport operator has the same meaning as defined. Because the definition of "operator" only refers to those holding a licence and operating a certificate, it is clear that this would not be applicable to private use drone operators due to the fact that they do not require a licence to operate the aircraft or operation certificate.

27 However, only commercial UAS/RPAS operators would be covered by this section.

28 "Aircraft" means any machine that can derive support in the atmosphere from the reactions of the air, other than the reactions of the air against the surface of the earth.

operation (such as surveillance or aerial photography) and advise clients to insure. But as it currently stands, only commercial operators of UAS/RPASs must take out insurance. It is recommended that private use operators should also be required to take out adequate insurance for the many risks associated with these types of aircraft.[29]

Strict liability: In terms of section 9 of the Aviation Act of 1923,[30] an aircraft owner was strictly liable for any surface damage caused by the aircraft. For instance, if a pilot carries out an emergency landing in a farmer's field and sets the farmer's crop alight, the owner of the aircraft is liable without fault.[31] The position is still the same in terms of section 8(2) of the current Civil Aviation Act.[32] The significance of strict liability for hull damage is that it can be insured against and as all manned aircraft can potentially cause significant surface damage, this is an essential risk that needs to be insured against.[33]

Drones, although significantly smaller and not carrying huge quantities of flammables such as fuel, may still cause surface damage. Furthermore, drones do carry batteries and as such are also a cause for concern as they can cause fires.[34] As with any other risk associated with drones, it is not sure whether technical or legal knowledge provides sufficient information on the extent of potential risks pertaining to drones and surface damage. It is submitted that this is an area that stands out as a potential point of conflict between drone owners, third parties and insurers.[35]

B. AUTONOMOUS VEHICLES

The answer is "no". As per the explanation in question 1 above, personal injuries caused by motor vehicles fall under the Road Accident Benefit Scheme, unless specifically excluded. There is no indication as to where self-drive vehicles will fit in, as the definition of ''vehicle'' in the Road Accident Benefit Scheme Bill means "a vehicle designed or adapted for propulsion or haulage on a road by means of fuel, gas or electricity, including a trailer, caravan, agricultural or other implement designed to be drawn by such a vehicle". It is therefore submitted that the Bill, once a statute, should either be amended to specifically provide for autonomous vehicles or should specifically exclude

---

[29] See Huneberg "On Drones, New Risks and Insurance" 2017 THRHR 586.

[30] Act 16 of 1923, now repealed.

[31] Neethling and Potgieter *Neethling-Potgieter-Visser Law of delict* (2015) 342–345.

[32] This specific section reads as follows: "Where material damage or loss is caused by (a) an aircraft in flight, taking off or landing; (b) any person in any such aircraft; or (c) any article falling from any such aircraft, (d) to any person or property on land or water, damages may be recovered from the registered owner of the aircraft in respect of such damage or loss, without proof of negligence or intention or other cause of action as though such damage or loss had been caused by his or her wilful act, neglect or default."

[33] See Huneberg "On Drones, New Risks and Insurance" 2017 THRHR 586.

[34] See Huneberg "On Drones, New Risks and Insurance" 2017 THRHR 586.

[35] See Huneberg "On Drones, New Risks and Insurance" 2017 THRHR 586.

these. If excluded, these vehicles should be regulated separately and compulsory insurance should be provided for.

Product liability insurance is available privately and policies depend on the kind of enterprise and risk. It is submitted that there is currently no difference between autonomous cars and any other products that may cause liabilities.

3. How do you envisage the future of personal lines in motor vehicle insurance in the next 5-10 years in your jurisdiction?
Comment: you may wish to comment on the future of motor vehicle insurance and the plans being made by the industry for new products

The future of personal lines in motor vehicle insurance might be expected to change significantly due to the introduction of autonomous vehicles but in South Africa, this does not seem to be something that will be implemented in the next 5-10 years. The reason for this is due to the fact that there are many challanges facing the introduction of these vehicles in South Africa. Firstly, South Africa has approximately 746 978 km of roads and only 158 124 km of these roads are paved, according to Wheels24.[36] The rest of the roads are either gravel or dirt roads in rural areas. Apart from the large number of rural roads, the main roads in cities like Johannesburg suffer from poor road conditions (including potholes and a major lack of road signs and street names) as well as vandalism to road signs. All of these factors would would hinder an autonomous vehicle's ability to navigate.[37]

Apart from the state of our roads, South Africa also has a large number of **unpredictable obstacles** for drivers to navigate. From taxis, to pedestrians, and even livestock, there are hundreds of obstacles which would confuse self-driving cars.[38] The taxi industry in itself would also be a factor hindering the use of these vehicles in South Africa. Uber drivers have faced many issues from the taxi industry and this may also be a concern for autonomous vehicles. In order for autonomous vehicles to be effective in South Africa, the country would need to first ensure that the infrastructure was in place to support these vehicles. This is a major concern for the implementation of autonomous vehicles in South Africa and may take many years to overcome.[39]

4. Driverless cars and autonomous vehicles apart, how do you assess the following technological developments that are expected to not only reshape the auto sector but also the insurance industry

[36] See http://blog.suzukiauto.co.za/blog/why-self-driving-cars-wont-work-in-south-africa.-.-.-yet
[37] See http://blog.suzukiauto.co.za/blog/why-self-driving-cars-wont-work-in-south-africa.-.-.-yet
[38] See http://blog.suzukiauto.co.za/blog/why-self-driving-cars-wont-work-in-south-africa.-.-.-yet
[39]See http://blog.suzukiauto.co.za/blog/why-self-driving-cars-wont-work-in-south-africa.-.-.-yet

around it?

(a) connected cars (i.e., Internet enabled vehicles, (IEV));

(b) automated driver assistance systems (ADAS);

(c) car/ride sharing;

(d) alternative fuel vehicles.

Comment: answers may include identifying the legal and regulatory regime and provisions in your jurisdiction.

Unless there will be dedicated legislation to regulate all these kinds of vehicles, it is expected that the following regime will apply:
For *damage caused to property* (damage to the vehicle), the *actio legis Aquilia* as described in question 1 above will apply, incorporating all the principles of Roman-Dutch law.

For *personal injuries*, the Road Accident benefit system will apply, unless the vehicle in question is not propelled by fuel, gas or electricity. It is submitted that this issue will in all likelihood receive attention as soon as driverless vehicles are licensed for road usage.

For *manufacturer's liability*, the Consumer Protection Act (CPA)[40] will apply. In this regard, it should be noted that section 55 of the CPA, imposes a statutory duty on manufacturers to provide consumers with safe goods. When such a statutory duty is allegedly breached, the following requirements need to be proved to establish the unlawfulness of conduct. Firstly, a claimant must prove that the relevant legislation provides grounds for a private law action in the event of a breach. Next, a claimant is required to prove that the provision was enacted for the benefit of a class of persons and that the claimant forms part of such a class. In this regard, a plaintiff should qualify as a "consumer" in terms of the CPA. It is further required that the harm and the manner in which the harm occurred must fall within the ambit of the legislation.

II. CYBER RISKS

5. Identify the concerns have emerged in your jurisdiction as a result of cyber risks. Is there any legislation in place or under consideration that might affect such risks?
Comment: possible matters include cyber-terrorism, hacking, computer or software failure and financial fraud.

[40] 68 of 2008.

The Electronic Communications and Transactions Act (ECTA)[41] was enacted:

"To provide for the facilitation and regulation of electronic communications and transactions; to provide for the development of a national e-strategy for the Republic; to promote universal access to electronic communications and transactions and the use of electronic transactions by SMMEs; to provide for human resource development in electronic transactions; to prevent abuse of information systems; to encourage the use of e-government services; and to provide for matters connected therewith."

This act applies to any electronic contract and in principle includes an insurance contract entered into electronically. In South Africa, low levels of literacy and limited access to computers have seen insurers resort to more traditional ways of entering into contracts with a result that insurance statutes still apply to the majority of insurance contracts.

Aspects pertaining to actual risks such as cyber-terrorism, hacking, computer or software failure and financial fraud are covered by the new Cybercrimes and Cybersecurity Bill. The object of this Bill is:

To create offences and impose penalties which have a bearing on cybercrime; to criminalise the distribution of data messages which is harmful and to provide for interim protection orders; to further regulate jurisdiction in respect of cybercrimes; to further regulate the powers to investigate cybercrimes; to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrime; to provide for the establishment of a 24/7 Point of Contact; to further provide for the proof of certain facts by affidavit; to impose obligations on electronic communications service providers and financial institutions to assist in the investigation of cybercrimes and to report cybercrimes; to provide for the establishment of structures to promote cybersecurity and capacity building; to regulate the identification and declaration of critical information infrastructures and measures to protect critical information infrastructures; to provide that the Executive may enter into agreements with foreign States to promote cybersecurity; to delete and amend provisions of certain laws; and to provide for matters connected therewith.

The Bill, once in force, will place an obligation on insurers to assist in the investigation of cybercrimes and to report cybercrimes. Cybercrimes are discussed extensively in chapter 2 of the Bill, and include inter alia unlawful securing of access, unlawful acquiring of data, unlawful acts in respect of software or hardware tool, unlawful interference with data or computer program, unlawful

[41] 25 of 2002.

interference with computer data storage medium or computer system, unlawful acquisition, possession, provision, receipt or use of password, access codes or similar data or devices, cyber fraud, cyber forgery and uttering, cyber extortion and attempting, conspiring, aiding, abetting, inducing, inciting, instigating, instruct-ing, commanding or procuring to commit offence.

Financial fraud, including insurance fraud, is still regulated by Roman-Dutch law and where such fraud is committed with electronic means, it is submitted that the Cybercrimes and Cybersecurity Bill will in future regulate the situation, with the additional requirements that financial institutions must co-operate to combat these crimes.

By defining these cyber crimes, South Africa will have a legislative regime that will make it possible for insurance companies to outline possible risks and write insurance policies to cover (or exclude) these risks.

6. How has the insurance industry responded to cyber risks? In particular:

(a) do property policies cover losses from cyber risks, or is special insurance required?

Special insurance is required. A typical cyber policy coves the following, namely:

- Data Liability - covering the damages and defence costs associated with a breach of personal or corporate data.
- Data Security - damage resulting from any breach of duty that ends in Contamination by Malicious Code of Third Party Data, improper or wrongful denial of access by an authorised Third Party to Data; the theft of an access code from premises, Computer System, or employee; the destruction, modification, corruption, damage or deletion of Data stored on any Computer System due to a Breach of Data Security and data disclosure due to a Breach of Data Security.
- The physical theft of hardware.
- Data Administrative Investigation - provides costs and expenses for legal advice and representation in connection with a formal investigation by a Data Protection Authority or other regulator.
- Data Administrative Fines - insurable fines and penalties obligated to pay to a government authority, regulator or data protection. authority for a breach of data protection laws or regulations.
- Notification & Monitoring Costs - provides costs and expenses of the Data User for the legally required disclosure to Data Subjects.

- Repair of the Company's and Individual's Reputation - reimbursement of costs incurred in relation to Reputational Damage due to a claim covered by this policy.[42]

(b) is insurance and reinsurance readily available?

Yes.

(c) are there any special restrictions imposed on cyber risks, e.g. event limits or deductibles?

Not by legislation. Parties may negotiate restrictions in their policies.

III. NEW TECHNOLOGIES AND THE INSURANCE PROCESS

7. To what extent have the availability of new technologies affected the way in which insurance policies are placed? In particular:

(a) has there been any effect on the traditional use of agents and brokers?

There are direct insurers who use on-line processes to transact. However this is not the norm in South Africa as many industries (such as funeral insurance) target lower income groups who do not have access to computers.

(b) has the underwriting process been affected by the availability of information, particularly big data, from sources other than the applicant for insurance?

The Protection of Personal Information Act (POPI Act)[43] aims to protect people from harm by protecting their personal information, which includes having their identity stolen or having unlawful access to their personal information. The Act also sets conditions for when it is lawful to process someone else's personal information. Essentially, if an insurance company seeks information on a potential policyholder, such information must be tendered by the policyholder and this Act prevents insurers from accessing personal information. That means that the underwriting process has not been affected by big data.

(c) has the means of providing information to policyholders changed significantly, e.g. are written documents provided or are policyholders directed to websites?

[42] See www.aig.co.za accessed 6 March 2018.
[43] No 4 of 2013.

Although there is an increasing drive to provide information electronically, many `south Africans still do not have access to computers and this means that written documents must be provided, unless clients choose to receive electronic communications.

8. To what extent is genetic testing regarded as important by life and accident insurers? Is there any legislation in place or in contemplation restricting requests for genetic information, and are there any relevant rules on privacy that preclude its disclosure?

Genetic tests are not carried out as a rule and a genetic test that was requested by a patient for purposes other than insurance constitutes a medical record. In terms of sections 14 and 16 of the National Health Act,[44] no medical record may be made available without the subject's explicit consent. It is submitted that genetic tests are too expensive to be used in determining future risks.

9. Has the assessment of claims been affected by the availability of data. In particular, are there any industry-wide arrangements in place whereby insurers can share information on fraud?

Yes, South Africa has the Insurance Crime Bureau. This organisation is a non-profit company dedicated to fighting organised insurance crimes and fraud. The organisation makes use of collective resources of insurance companies, law enforcement agencies and other stakeholders to facilitate the detection, prevention and mitigation of insurance crimes as well as assist in the prosecution of repeat offenders and fraudsters through ongoing insurance fraud investigation.[45] Over the years, various initiatives have been implemented by The Insurance Crime Bureau to address organised crime in the industry as well as a number of educational efforts aimed at the public to create awareness of insurance fraud scams. This system allows the members (insurers, specifically) to benefit from collaborative experiences through data sharing. This idea of data sharing is fundamental to identify and curb fraud. Insurers can become members on a voluntary basis.[46]

The ultimate goal of The Insurance Crime Bureau therefore, is to create a joint initiative for the whole insurance industry and other related stakeholders to address crime and fraud through the sharing of information.[47]

Furthermore, The Insurance Crime Bureau also provides a platform for the public to safely and anonymously report fraudulent activities or suspected insurance crimes through the toll-free Insurance Fraudline.[48]

10. Are there any other ways in which the new technologies have affected the insurance process in your jurisdiction?

No.

---

[44] 61 of 2003.
[45] See https://www.saicb.co.za.
[46] See https://www.saicb.co.za.
[47] See https://www.saicb.co.za.
[48] See https://www.saicb.co.za.

IV. OTHER NEW TECHNOLOGY RISKS

11. Are there any other particular risks from new the new technologies that have been identified in your jurisdiction? If so, is there any legislation in place or under consideration to regulate them?
No.