Cloud LSVA

Large Scale Video Analysis

EUROPEAN COMMISSION
DG Communications Networks, Content & Technology

Horizon 2020 Research and Innovation Programme
Grant Agreement Nr 6880099

Report on data legal requirements and implemented data protection approaches

Deliverable no.	Deliverable 2.4
Dissemination level	Public
Work Package no.	WP2
Main author(s)	Professor Raymond J Friel ULIM
Co-author(s)	Finbarr Murphy (ULIM)
Version Nr (F: final, D: draft)	V0.3
File Name	Cloud LSVA Data Protection Deliverable_v1.0
Project Start Date and Duration	01 January 2016, 36 months

Project funded by the European Union's Horizon 2020 Research and Innovation Programme (2014 – 2020)

Document Control Sheet

Main author(s) or editor(s): Professor Raymond J Friel ULIM

Work area: WP2

Document title: Cloud LSVA Data Protection Deliverable_v1.0

Version history:

Version number	Date	Main author	Summary of changes
v0.1	01.02.2017	R.J. Friel	Table of Contents
v0.2	15.02.2017	R.J. Friel	Inputs to all sections
V0.3	17.02.2017	R. Murphy	Internal review and inputs to sections
V0.4	24.02.2017	R.J Friel	Version after external review

Approval:

	Name	Date
Prepared	Professor Raymond J Friel ULIM	20/02/2017
Reviewed	Phil Jordan IBM	22/02/2017
Authorised	Oihana Otaegui	27/02/2017

Circulation:

Recipient	Date of submission
EC	28/02/2017
Cloud LSVA consortium	27/02/2017

Legal Disclaimer

Contents

Executive Summary

The aim of this project is to develop a software platform for efficient and collaborative semiautomatic labelling and exploitation of large-scale video data solving existing needs for ADAS and Digital Cartography industries.

Cloud-LSVA will use Big Data Technologies to address the open problem of a lack of software tools, and hardware platforms, to annotate petabyte scale video datasets, with the focus on the automotive industry. Annotations of road traffic objects, events and scenes are critical for training and testing computer vision techniques that are the heart of modern Advanced Driver Assistance Systems and Navigation systems. Providing this capability will establish a sustainable basis to drive forward automotive Big Data Technologies.

As part of Cloud-LSVA project, the objective of WP2 is to examine scene recording, network and Cloud based data management. In particular deliverable 2.4 requires a report on the data legal requirements and implemented data protection approaches.

Following an extensive literature review and legislative and jurisprudential research on the impact of data protection regulations as they apply to autonomous and semi-autonomous connected vehicles specifically using the technology under development in Cloud-LSVA, this report makes the following findings

Cloud-LSVA will acquire personal and non-personal data. The former is the subject of this paper, while the latter (which may have significant commercial value) falls outside the scope of the terms of reference.

Cloud-LSVA will acquire personal information as part of its data acquisition technology.

That personal data must be obtained, secured and utilized in strict accordance with relevant EU and national data protection frameworks.

That the current EU directive permits national variations in implementation and sets a minimum level of protection that must apply in all member states.

Simply put acquired data must be obtained with informed consent, used only for the purposes for which it was acquired and deleted after that purpose has been completed.

There is an implicit assumption that the storage of such personal data will have sufficient security as is consistent with the potential risk of breach. That level of security is beyond the scope of this deliverable but ISO standards are available.

Cloud-LSVA project has two distinct phases: research and implementable technology. Although it is possible to distinguish these two phases for data protection issues, the project must be cognizant of “privacy by design” and the use of Privacy Impact Assessments as part of best practice.

In the research phase, although there is no general exception to data protection provisions that arise to data collected for research purposes, there are some exceptions to the general principles. Outside of this, data protection provisions should utilize full consent by way of contract provisions for participants in the research.

In the implementable technology phase, it should be noted that the project will be completed at the same time as the provisions of the EU General Data Protection Regulation takes effect in 2018 and in pursuing privacy by design this is the standard to which the project should look to.

The EU General Data Protection Regulation will significantly strengthen data protection provisions including the requirements for a valid consent (unambiguous) and liability for data processors as well as controllers together with stronger penalties and sanctions.

The acquisition of data where consent can be given must include not merely owners or registered users but also other users. This will require appropriate visual or audio notices regarding data protection issues. It will still require anonymization of personal data and the use of contractual provisions to scope the risk. In that regard the Global
Automobile manufacturers guiding principles are instructive.

The acquisition of data where consent is not possible, for example other road users, should be addressed by analogy to CCTV cameras, that is the information will solely be used for a socially desirable purpose (here the safety of human life) and for no other purpose. Again, anonymization and secured storage of the data is a pre-requisite.

Internationally, a guiding principle which appears to be emerging is that there needs to be higher levels of data protection where the technology is mandatory as distinct from optional.

Given the mobile nature of the automobiles, the location and transmission of data is likely to have an international dimension. If this all occurs within the EU the issue is relatively easily dealt with. If it occurs outside of the EU, then it must be in accordance with general agreements such as Privacy Shield, or perhaps more importantly significant use of the model contract clauses that establish similar EU protections for information held outside the EU.

New developments outside of these frameworks will test the limits of privacy. Case law is emerging concerning potential economic harm. Some member states are implementing counter-terrorist measures that will impact on data protection.

All of this is reflective of the changing environment that the research and introduction of this technology is experiencing.

1 Introduction

The purpose of this document is to provide a comprehensive yet accessible survey of the data protection framework as it applies to the technology required for autonomous and semi-autonomous vehicles generally and Cloud LSVA technology specifically.

The use of the word 'accessible' is designed to capture the fact that this is not designed to be a high level, abstract and conceptual legal paper aimed at a professional and academic legal individual familiar with various legal taxonomies. Yet neither is it designed to mimic one of the many over-simplistic approaches found on the internet aimed either at attracting business or spurring agenda driven groupings in favour of or opposed to developing technology on ideological grounds.

Instead the deliverable is written in a style and format designed to be usable by the differing discipline specialists likely to be involved in the development of this technology. This is no easy task and to claim success would be to demonstrate hubris likely to lead to a fall. It would be better to say that at least this was the aim of the deliverable and to leave the judgment of its success or failure on those who read it.

There are however two caveats that need to be addressed here. The preceding year (2016) has seen rapid developments across the data protection framework and the technology involved in autonomous and semi-autonomous vehicles. The pace of change has been significant. In fact so significant that the already unstable ground upon which data protection and this particular technology sat only 2 or 3 years ago, has become even further unstable. Much of this deliverable has had to deal with this uncertainty in a manner which brings some stability to the area but which cannot hide entirely the buffeting winds of change blowing through this sector. In some instances the only option has been to resort to speculative assumptions as to how things will develop. At each stage, best efforts have been made to reduce the amount of uncertainty and minimize the speculative element, raising the probability that it represents the final outcome. Often there is an expectation that the law, and its practitioners, have failed if they cannot provide full certainty. It may surprise some to say the law is a work in progress and that is why it is called the practice of law. In many ways the law shares the same scientific voyage from hypothesis to proof in a journey that never seems to end.

The second caveat is that the technology that we are dealing with in autonomous and semi-autonomous vehicles, and in particular connected vehicles which communicate with each other, local infrastructure and the cloud, relies upon the acquisition and analysis of massive amounts of data. That data will fall into many categories but our concern here is with only one type of data: data likely to lead to the identification of a human (or as the 1995 Directive de-humanisingly terms it: a data subject).

Although there is no evidence to back up this particular statistical claim, one suspects that the amount of personal data likely to identify an individual will be far outweighed by other categories of data

collected. But it is only personal data that this deliverable deals with and for which there exists a legal and regulatory framework which governs how that data must be acquired and handled.

The non-personal data is free from any such limitations or restrictions as to use. Yet in fact that data is probably and potentially of far greater commercial value. Non-personal data such as the weather conditions at the time of an accident, the operating temperature at which a vehicle component failed may provide immense commercial insights into innovation and product change. Product liability insurers for example may find mass data on the performance of a particular vehicle component hugely valuable in setting premiums or determining whether a recall is the only option.

Non-personal data in many ways therefore differs only in that it does not have a formal regulatory framework by which it is controlled. But given the potential value, it seems as a matter of commercial reality that apart from the consent issue, which is crucial in personal data, non-personal data should at least be sufficiently secure in its transmission, storage and retrieval as personal data. Moreover this non-personal data may constitute some Intellectual Property Right. Remember non-personal data is the equivalent of a large sum of cash: it is as deserving of protection as personal data. The failure to protect the monetary value that might reside in non-personal data may leave an entity open to legal liability for breach of duty. However, that is beyond the scope of this deliverable. We are confined to deal only with data protection rules as they apply to personal data.

In summary

- Both the law and technology underpinning autonomous and semi-autonomous vehicles is in a rapid state of flux creating uncertainty
- This work only deals with personal data acquired as a result of this technology; personal data is that data likely to lead to the identification of the individual.
- Personal data is covered by a well-established legal and regulatory framework.
- Non-personal data acquired as a result of this technology is not covered but it may have significant commercial value and should therefore be the subject of similar protections based on a duty of care.

With those caveats in mind we turn now to deal with the various issues that arise with respect to personal data.

2 Background to Data Protection – the fear agenda

Privacy is an essential part of human nature since time immemorial. Although few can deny this fact, the attempt to capture what it means in operation is not without difficulty. Each of us have differing levels of what we consider public versus private information. Indeed even within that context, we have

differing levels of acceptability as to who should have access to our private information: the more intimate a relationship, the less we regard as private. Some of that need for privacy is driven by fear. We tend to regard that as private which is likely to cause us harm in our professional or private lives. We will reveal more when that fear is counterbalanced by the advantages of such a revelation. For example, a person may hide an affair from their spouse but will reveal it to their doctor in the interests of their own health. Although coupling privacy with fear may seem unduly negative, it is not meant to carry any particular connotation other than in dealing with privacy issues, particularly as they arise in autonomous and semi-autonomous vehicle technology, it would be wiser to recognize one of the primary drivers of privacy concerns by the public.

3 Privacy as an International Human Right

This human need for privacy finds expression in major international Conventions, Treaties and national Constitutions and laws. And it does so in a way which both reflects the illusory nature of what information should be regarded as private and from whom. For example the European Convention on Human Rights protects privacy based on the right to a family life (Art 8.1). But it does not specifically define what that privacy relates to, although in Art 8.2 it does highlight one of the key parties who we as citizens fear will most likely invade our privacy to our detriment: the state.

It is no co-incidence that the vast bulk of formalized privacy protections emerge after World War II. The Nazi regime excelled in acquiring personal information from its citizens and conquered people in a scientific and comprehensive manner never before seen. The Nazi's understood that information is power and both amassed and filed as much information as was then humanly possible, deploying huge financial and human resources to this venture. In doing so they too were driven by fear. Fear that without this information their grip on power would be lost. And this fear resulted in creating even more fear for the people they ruled: that their personal information could be used against them. The net result: an ethos within public institutions that peace and security required access to all areas of their citizen's information and a belief in the citizenry that all information acquired by the state would ultimately be used against them in harmful ways. Long after the Nazi's would be vanquished, the element of fear, both by the state and its citizens, to privacy would drive legal and political discourse for decades to come.

4 EU Data Protection

4.1 Directives explained

In an EU context, national and international concerns found expression in the Data Protection Directive. Simply put, a Directive is an order by the EU to its member states requiring that certain objectives be achieved but leaving the member state free as to how this should be achieved. Perhaps the best example of this would be through the issue of equal pay between men and women for like work. An EU Directive might mandate that each member state should achieve the objective of equal pay between men and women but in doing so the state is free as to how this is to be done. Our initial reaction might be to assume that it is achievable by raising the pay of women to match that of their male colleagues. But of course the objective could also be achieved by lowering the pay of their male colleagues to match that of their female counterparts. Both approaches achieve the objective but in radically different ways.

The concept of the Directive at EU law must be contrasted with an EU regulation, and we will return to that distinction later. But before leaving the analysis of a Directive as a legislative tool, there are two further issues that must be addressed. First, although Directives are couched in relatively vague terms, some Directives may have a sufficient level of detail that there is in fact very little discretion in the member state. For example, in the above example the Directive might have said that it was required to create equal pay between men and women by raising the pay of women to match their male counterparts. So the terms of the Directive may be more prescriptive of its objective, leaving little choice in how it is to be achieved.

Second, Directives normally establish a floor or base-line minimum of an obligation on the member state which is often free to add to that if it is wishes to do so. For example, in the equal pay example above, a member state may in addition to legislating for equal pay, provide additional rights beyond equal pay such as a minimum wage. So long as what the state adds does not defeat the purposes or objective of the Directive this is permissible.

Finally, it should be noted that although Directives usually require national implementing legislation such as an Act in order to be incorporated into the national legal system. Without that national enactment, the Directive is not yet law within that member state. However, an EU citizen may in limited circumstances acquire rights under an EU Directive that has not been enacted into national law where the Directive is clear and unconditional and the time for enactment has passed.

5 EU Data Protection Directive

5.1 Definitions and Terms

Participants in the Cloud LSVA project need to be aware that the concepts behind data and data protection are legally defined. As with all legal definitions, the intention is to provide an exactness from which certainty as to application to events can be ensured. Having said that, all wording carries inherent vagueness and uncertainty but for the purposes of this document we can provide relevant definitions and commentary as to potential application to the Cloud LSVA project.

Data Subject means an individual from, or about, whom the data was collected.

Cloud LSVA: this will cover any person who is recorded by the technology including other road users, pedestrians, people in buildings adjacent to the roadway etc.

Data includes information that is being processed by means of equipment operating automatically in response to instructions given for that purpose, or which is recorded with the intention that it should be processed by means of such equipment.

Cloud LSVA: the recording technology which captures video footage for analysis will fall within this category.

Personal data means data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

Cloud LSVA: this will restrict the application of data protection to that video footage which presents a clear picture of the data subject. It is not necessary to be in a position to identify the data subject at the time the recording is either made or analysed. The issue is whether the data controller is likely to come into possession of other information with which to make an identification.

Sensitive personal data means personal data as to the commission or alleged commission of any offence by the data subject, or any proceedings for an offence committed or alleged to have been committed by the data subject

Cloud LSVA: This may arise where the video recording captures an individual in a suspected criminal act (a recording of an individual mugging a pedestrian) or which might be used in evidence to support a prosecution based on the alleged criminal act (a recording of an individual running from away bank robbery with a bank money bag).

Data controller/processer is a person (natural or legal) who controls the contents and use of the data, including one who processes the data at the request of the data controller.

Cloud LSVA: For the purposes of this programme, the controller would be the entity who directs the use to which the video recordings are to be put. It is not a requirement that the controller have access to the data or process it themselves. It would thus include 3rd parties who might process the information. Example: video recordings are sent back to a central database owned by X who in fact has contracted out the analysis of the recordings to Y. X is the data controller and Y is the data processor.

*Processing, of or in relation to information or data***,** means performing any operation or set of operations on the information or data, whether or not by automatic means, including-

(a) Obtaining, recording or keeping the information or data

(b) Collecting, organising, storing, altering or adapting the information or data, (c) retrieving, consulting or using the information or data,

(d) Disclosing the information or data by transmitting, disseminating or otherwise making it available, or,

(e) Aligning, combining, blocking, erasing or destroying the information or data, and, cognate words shall be construed accordingly.

Cloud LSVA: It is fairly clear that the project will involve processing any data obtained.

Summary

The Cloud LSVA programme will clearly involve the acquisition of data, including some personal or sensitive data although this is less likely. That data will by definition be subject to the control of one of more persons (including legal persons such as companies) and will also be the subject of processing within the meaning of the provisions.

5.2 Legal Obligations on data controllers and processors

Data controllers/processors must comply with the following

- Obtain and process information fairly and compatible with the purposes for which it was given.
- Data should be obtained and processed only the extent that it is adequate, relevant and proportionate to the purpose it was obtained for.
- Store such information safely and securely.
- Retain the information no longer than is necessary for the specified purpose/s.
- Provide a copy of any relevant information on the data subject held by the data controller/processor

For the most part these are self-explanatory. However, it should be noted that the better view is to take a narrow, restrictive interpretation of the conditions, thus when faced with a choice, Cloud LSVA must take the approach which provides the greatest level of data protection. Making decisions based on an 'arguable case' is not appropriate.

6 How Cloud LSVA differs from traditional data protection models

The basic thrust of the legal protection on data revolves around the classic situation where the data subject voluntarily provides the data to the data controller. Thus most of the rules concern issues surrounding the consent of the data subject, limiting the data that is acquired to the minimum necessary to achieve the stated objective of the data controller, and strictly prescribing the use to which the data is put and the ability to share that information for purposes other than that disclosed at the time of acquisition. Finally, it permitted the data subject to view the personal data held with a right to redress inaccuracies.

Cloud LSVA by design does not seek, nor could it reasonably endeavor to so seek, the prior consent of potential data subjects and therefore the application of the existing rules cannot be a straightforward matter. However this is not the same as saying the rules do not apply to Cloud LSVA but simply that they must be modified in application. The basic principles behind data protection remain as relevant to Cloud LSVA as they do the classic data acquisition model.

What then are the basic principles?

- Data protection is to be built in at every phase of the design process
- Ensuring that protection of data is the default setting for all design choices
- Given the non-consensual acquisition of data, the highest level of protection possible
- Clear rules with respect to processing and sharing of the data with external actors

It is also important to be aware that the level of data protection issues will escalate as Cloud LSVA goes through its design phases and that needs to be addressed within each stage

Development Stage	**Level of data protection issues**
Test track development	Low
On road pilot stage	Medium
Commercial pre-production	High

Note however that even within a closed test track development, data protection issues are low, not non-existent.

Returning to the Directive on Data Protection, simply put it requires member states to enact legislation which regulates and controls the acquisition, storage and use of information to a minimum standard. The Directive is relatively specific such that there is little discretion in how a member state may achieve the over-riding objective of data protection.

There are a number of key principles to be found in the Directive which are of relevance to Cloud LSVA.

First, for the most part, the acquisition of information, or more technically data, is to be undertaken with the consent of the individual.

Second, that consent can only be effective if it is an 'informed' consent. Essentially, this means that the individual should know why the data is being collected, what use will be made of the data, where it will be stored and who will have access to it and for how long. Armed with this information, the individual is in a position to make an informed decision.

Third, the data acquirer should only obtain that data which is essential for the stated purpose. The data acquirer should not acquire more information than is necessary. There is therefore a minimalist approach to data acquisition.

Fourth, the captured data should be used only for the purposes stated and for no other reason. There is therefore a restricted approach to data usage.

Fifth, access to the data should tightly controlled so that only those parties who have a defined need to access the data are allowed to do so. There is therefore a secured access approach to data storage.

Finally, the data should be stored only for so long as is required to achieve the purpose for which the data had been acquired. Once this has achieved the data should be safely destroyed.

One way of looking at this would be to summarise data protection into four main principles as set out below:

Data Protection Directive Principles

- Informed Consent to the acquisition of data
- Minimalist approach to the acquisition of data
- Restricted use and secure storage of acquired data
- Timely destruction of acquired data

The Directive goes on to do other things such as the establishment of national agencies to enforce these provisions, but we are not concerned about these at this point.

Without dealing with it fully at this stage, it is clear that the technology behind Cloud LSVA does pose concrete challenges with respect to these principles:

- First, on the issue of informed consent, the recording of the scene around the vehicle will of necessity involve non-consensual acquisition of data.
- Second, the extent of the data that needs to be acquired appears to more comprehensive than might be assumed and the granularity of the required video data appears of a higher order than simple pixilation would achieve.
- Third, the acquired data will be communicated over V2C and V2V networks and both data transmission networks and cloud data storage will provide challenges for robust security frameworks.
- Finally, as Cloud LSVA involves continued computer learning by building up ever larger case scenes, it is unclear at what point the data can be deleted.

One of the issues that arises with respect to Cloud LSVA technology and the Directive is the changing technology on data acquisition and interrogation. The Directive represents an era when data acquisition was primarily paper based, predominantly provided by the data subject themselves and thereby gave an opportunity to the data subject to give or refuse consent.

None of these constraints apply with Cloud LSVA technology whose very nature will require the acquisition of non-consensual data. Moreover the scale of data which is to be acquired, stored and analysed is of exceptionally large volumes. In one way, the very scale of the information might be expected to provide a degree of comfort from the fear inherent in data abuse.

Although the Nazis were excellent in establishing processes to acquire and store data, a skill that for example would continue in East Germany with the Stazi secret police, it became obvious that excessive information is not that powerful unless it can be easily retrieved for a specific purpose. The limitation on data use was not its acquisition but its retrieval. Thus most of the information acquired would never be used due to the practical limitations on retrieving and cross-referencing the data. In the success of acquiring information lay the seeds of its limitation: inability to use ever increasing volumes of data.

Modern technology has not only exponentially increased the quantum of acquired and stored data but also exponentially increased the speed by which that data can be interrogated and relevant information extracted and used for specific purposes. The safety of limited use of ever increasing quantities of acquired data is now well and truly gone.

Certain events have a transformative effect on the nature of society. The advent of the Nazis impacted on international and national laws for decades after their demise. Today, new technology is creating a transformative environment for the implementation of Cloud LSVA technology. The fears encapsulated in the data protection provisions of the Directive are now being changed as a result of huge advances in technology never envisaged at its creation.

In summary

- The EU Data Protection Directive is premised on a limited technology environment.
- New technology, including Cloud LSVA, requires new approaches

7 The EU General Data Protection Regulation

As a result, the EU has enacted a new data protection Regulation which will come into effect in 2018. A Regulation differs from a Directive discussed earlier in that it is binding on member states both as to the objective and the manner in which it is to be achieved. It is highly prescriptive and, unless specifically provided for, does not confer any discretion on the member state as to its application. In fact, not only is enabling legislation at national level not required, any attempt to 'nationalise' the directive through an implementing measure is prohibited. The Regulation provide rights to all EU citizens as soon as it becomes effective.

The GDPR represents a step change that reflects the transformative nature of data acquisition and retrieval technology. However it is reflective of the public fear that such technology has with respect to their privacy rights. In this way, the GDPR may not be conducive to the technology in Cloud LSVA.

In brief, the new GDPR provides significant enhancements to the safeguards which were present in the earlier Directive.

- First, the issue of consent has been strengthened to ensure that not only is the consent informed but that it is unambiguously given. It essentially removes implied consent as a valid consent.
- Second, it provides for the withdrawal of consent, a new innovation.
- Third, it extends the responsibility for data protection wider so as to include not only those who control data but also those who process it.
- Fourth, tightens up the control of data across borders by requiring in certain situations the presence of agents within the EU for data held by foreign entities.
- Finally, it significantly increases the penalties and sanctions that arise on breach of data protection rules, now calculated as a percentage of turnover.

The GDPR also provides for additional powers, co-operation and liaison between national agencies.

For Cloud LSVA, these new changes will provide additional challenges

- First on consent, the acquisition of non-consensual data will prove problematic and resort will have to be made to alternative models such as apply in CCTV and drone photography.
- Second, clear delineation of data controllers and processors will be required as will increased contractual allocation of risk and responsibility between the various actors in the technology.
- Third, given the mobile nature of automobiles which regularly cross borders, greater care needs to be taken both with respect to where the data is being acquired and where it is being sent. The departure of the UK from the EU for example may have substantial repercussions for EU visitors to that country using Cloud LSVA technology
- Finally, risk factors arising from the increased financial sanctions for data protection breaches will require enhanced re-evaluation of transmission, access and security for data by both processors and controllers.

8 Cloud LSVA Project and the Data Environment

This project provides additional challenges above and beyond that which arise naturally from the technology. First, the technology represents a dramatic fault line between two competing societal imperatives. On the one hand, increasing autonomous or semi-autonomous automobile technology holds out the prospect of increased public safety, lower incidence of death and personal injuries from road traffic accidents and a smarter more efficient transportation infrastructure. On the other hand, this technology requires immense data acquisition and analysis when the public mood is highly skeptical of the potential for abuse of this data.

Evidence of this societal mood is to be found in the EU purported introduction of eCall technology. This technology is to be a mandatory feature car sold within the EU from 2018 onwards. Simply put eCall is a facility which will enable a vehicle which has become disabled as a result of an accident to contact the emergency services and direct them to the location of the vehicle to provide medical services to injured occupants. The system is designed to be dormant until activated as a result of a crash. It will provide for quicker and more efficient use of first responder services such as ambulance and para-medics. The speed with which medical intervention occurs in these types of injuries has a significant impact on survivability and recovery outcomes for injured citizens. As an analogy, more soldiers survive in modern warfare because the Army is now able to provide timely access to medical attention with rapid helicopter extractions of wounded personnel. In that way, eCall is a positive intervention.

However, there is evidence of public resistance to this technology. The basis for this resistance is the fear, unfounded, that the technology will be used generally to track the vehicle and its user. That fear is based on the realization not merely that the technology to track the vehicle exists but there is complementary technology to interrogate the stored data and retrieve a record of the vehicle movements.

The fear is unfounded – the system is not operative until a crash is detected. However, it is interesting to note that people are willing to sacrifice safety to avoid privacy violations. In a head to head battle between personal safety and personal privacy, safety may not always win.

Second, the technology being used in Cloud LSVA is part of a general transformative technology for which society and the law is ill-prepared. Data protection law, as all other legal constructs, uses a paradigm case scenario through which rules are created, analysed and applied. In contract law for example, the primary paradigm consists of two people equally met discussing the sale and purchase of a horse who is also present. The law which enables that transaction to occur is then applied on a universal level and the simplicity of the transaction results in modifications to the rules when it encounters the reality of new factual situations. Thus contract law responds to the introduction of new technology, such as the postal system by modifying the rule on when an acceptance occurs to being the moment it is posted which is the opposite of that in the original paradigm where it is the moment the acceptance is heard or received. As new technology emerges, for example faxes, emails etc., the law adapts to the changing impact on the paradigm.

For data protection, the paradigm is that of the citizen who fills in a form providing personal and other information to another who is in a position of dominance over the citizen (such as a government agency or financial institution) and who has the capacity to use that information incorrectly to the detriment of the citizen. The legal construct is to empower the citizen through consent and disempower the dominant party through restriction on acquisition and use of the data acquired.

Cloud LSVA technology alters the paradigm since the aim is to acquire, primarily non-consensually, data to protect the citizen and for which the potential for detriment to the citizen is low.

One question that arises of a fundamental nature is whether or not the data protection paradigm is actually relevant to Cloud LSVA technology which might be deserving of its own paradigm. For example, should transportation technology be exempt from data protection rules and instead by the subject of sui generis rules applicable to transportation only. This is a wider issue than that posed in this project but is worth mentioning. On the other hand, as stated above, it is not clear that the public has an appetite to surrender privacy for safety.

The net effect is that Cloud LSVA is taking place within an uncertain legal framework which is currently uncertain and too vague to resolve the many conflicting imperatives.

Third, to add to that uncertainty the current rules such as they are, are about to be replaced by new rules in 2018. These new data protection rules are still not designed with Cloud LSVA technology in mind and so are also limited in terms of usefulness. However the real issue is that the project will span two different legal regimes. Research will be conducted mostly under one regime and implementation would take place under a different regime. And that leads to the next issue of concern.

Fourth, the project itself divides naturally into two distinct phases. The initial phase is the research phase which is currently underway. At the end of that research process, the aim presumably is to be in a position to provide implementable technology to the market. This division which previously would have been accommodated simply by continuing the research and then back fitting data protection provisions is no longer appropriate. Today, the emphasis is on integrating privacy issues in the design process.

There is considerable merit to this approach, and best practice demands it use. However, it poses additional tensions between scientists and engineers who seek solutions to a problem (how can we make the car engage in autonomous braking) and the lawyers who seek to ensure that the range of solutions to the problem is limited in order to be consistent with a law that itself is not clear (for example what is the lowest level of video quality required to achieve autonomous braking). Although well meaning, privacy by design may limit technological advances and implementation and certainly has the potential to limit the research phase of Cloud LSVA.

Finally, the implementation phase of Cloud LSVA may take place in a revised transportation risk/liability environment. If as is possible, society may choose to rebalance safety over privacy, given the enormous financial and personal costs arising from automobile accidents when compared to data breaches, it will require a new and dedicated framework. Any such framework runs the risk that the research of privacy by design which occurred under rules which had a different priority, may result in more costly designs that protect privacy issues that no longer require the same level of privacy in the new framework. As a corollary, a new framework may impose other restrictions that were not considered relevant under the previous privacy framework.

In summary

- First, competing societal imperatives: safety versus privacy. In that conflict, safety imperatives may not always supersede privacy concerns.
- Second, an uncertain legal environment which was designed for an era where the impact of new data collection and interrogation technology was not as advanced.
- Third, the whole area of data protection is in the process of change resulting in two differing legal regimes applying to the research and implementation phase of Cloud LSVA technology.
- Fourth, a research environment that requires privacy by design despite a lack of clarity about exactly what that privacy means in the context of semi-autonomous or autonomous vehicles.
- Finally, if a new regulatory framework for autonomous and semi-autonomous vehicles emerges it may make both make some limitations on the technology redundant while also exposing gaps in the technology under the new regime.

9 Specific Cloud LSVA application

9.1 Research Phase

Before dealing with this issue in more detail, a word of warning. Best practice would indicate that a privacy impact assessment should be undertaken, particularly given the extent to which data acquisition and use forms a key element to the technology. Although there is no legal requirement for this to be done, it is indicative of best practice in this area.

In the research phase of the project Cloud LSVA will be minimally impacted by the GDPR as it will not take effect until 2018 towards the end of the project pipeline. However, it will (a) be subject to the Directive which continues in effect and (b) should consider the implications of GPDR as part of the design by privacy.

With respect to the existing data protection provisions, any research conducted within this framework needs to comply with the general principles under the Directive mindful of the fact that national laws of the member state may add to the general protections available under the Directive. For example, the acquisition of data consistent with the Directive may be prohibited by the law of the member state where the research is taking place. Some jurisdictions have enhanced data protection provisions which may be even more restrictive than the existing Directive or indeed the provisions of the Regulation.

What then are the existing provisions at EU level which Cloud LSVA needs to be aware of? Research conducted by the project needs to ensure compliance with the provisions of the Directive and in particular should be careful in securing an informed consent of all participant involved in the project. Although involvement in the project would in all probability give rise to a presumed consent to the acquisition of data and limited usage by third parties, there is no doubt that it would be advisable to secure explicit consent from any participant in the project which outlines the potential for personal data to be obtained and details the purpose for which it is to be used and the duration for which it is to be held.

It should be noted that such informed consent needs to be obtained not only from direct participants to the project but in two other situations as well. First, other data subjects who are not involved in the project also need to give their consent. For example, if the test vehicle is acquiring data while on a test track, other users of the test track, for example maintenance or other support workers should also give the relevant consent. In many cases a generic consent for these data subjects may be in place but it should be checked to ensure it covers this type of activity.

Second, the use of third party material, particularly videos should only be used subject to an explicit contractual agreement that the data was secured in accordance with the Directive or national provisions and that consent to its use by a third party has been given. It should be noted that under the Directive it

is not necessary that the original consent given included a research purpose, so if the consent for example was provided for training purposes, it can be used for research purposes despite that not being expressly mentioned in the original consent.

Even where this is the case, any video or other data which has the potential to identify a data subject should be removed to the extent that it is not necessary for the research purpose. A classic example would be a picture or video which contains the license plate of a vehicle. Even if the data subject has consented to the initial data acquisition, the consent does not extend to information not necessary to the task. If the picture or video is being used to assess spatial requirements for autonomous technology, the license plate is not a necessary requirement for that task.

Once consent has been established, this will provide the framework within which the data can be used. However, that data must be secured from inappropriate access or use outside of that to which the consent has been given. Contractual frameworks in the consent process can seek to limit the consequences of such a breach but it is important there is sufficient security in place to protect the data from inappropriate or unauthorized access. Inappropriate access would be access by someone who has a right to access the material but does so for a reason unconnected to the project. For example, X accesses a video in order to identify a data subject. No consent would be asked or given for such a purpose so although X can access the material, X has committed a data breach due to inappropriate purpose.

Unauthorized access either by a participant of the project who does not have the right to such access or by a third party who hacks into the system must be guarded against. The former can be dealt with by internal protocols as to who has access and requiring them to record, even if only in their own notes, the purpose of the access. The latter requires a level of security commensurate with the dangers of a potential breach. As the dangers involved in breach are relatively low, the security level is not required to be excessive. However, security issues are not part of this deliverable and so are only raised as potential issues without fuller treatment.

Finally, as much of the data acquired in the research appears to be intended as part of a bank of case scenes within which the systems can engage in deep learning, this too needs to be addressed within the contractual consent framework in terms of the duration of storage of the data, although again data for research purposes can be retained indefinitely but only for the research purpose. Beyond that consideration should be given to additional anonymization of the data if possible the longer the data is being held.

<u>In summary</u>

- Cloud LSVA research will be primarily conducted under the EU Directive although the GDPR may impact towards the end.
- The EU Directive is a base line which national rules may add to. Participants should ensure compliance with local member state laws.

- Under the Directive Cloud LSVA should ensure full compliance by
    - Contractual consent frameworks of an explicit nature for participants and any non-participant data subject.
    - Contractual consent framework assurances for 3rd party data including post acquisition anonymization of data where relevant
    - Data minimization in general to that which is necessary to the project
    - Secured system for access of data by participants
    - Security systems to prevent unauthorized 3rd party access to a standard commensurate with the potential harm from data breach.
- Finally, consideration to undertaking a Privacy Impact Assessment analysis should be undertaken.

9.1.1 Privacy by Design in the Research Phase

As the outcome of the research project involves technology likely to be introduced under the new GDPR provisions, it is important that at all stages the significance of this Regulation forms an integral part of the research evolution. It is inappropriate to assume that data protection measures can be added on afterwards in a manner which is consistent with the Regulation.

What then are the primary features of the GDPR as pertain to Cloud LSVA and 'privacy by design?'

9.1.2 Consent

The GDPR significantly strengthens the consent requirement of data subjects. From 2018, the consent must fully informed, explicit and unambiguous. It virtually brings to an end implicit or assumed consent. It will be for the data controller to prove that the consent was (a) obtained and (b) was based on full information. To that extent, privacy notices will need to be significantly strengthened. It should also be borne in mind that the GDPR requires that the language used in privacy notices or consents is plain and intelligible. Although the GDPR provisions indicate that consents and privacy notices may need to be lengthy, it is also clear that neither the length nor the terminology should prevent the data subject coming to a true consent.

As Cloud LSVA will record vehicle telemetry and will communicate this either V2C or V2V (or indeed V2I) it will require the consent of the driver. Where the driver is the owner this will be achieved through an initial contractual notification and consent procedure which will not impact on the technology. These consents will in best practice be governed not only by the GDPR but also by industry standards which may provide even greater protection. For example in the US, there is a Global Automakers General Principles on Data Protection. This provides a series of general guidelines with respect to Cloud LSVA technology:

Transparency

Participating Members commit to providing Owners and Registered

Users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of Covered Information.

Choice

Participating Members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information.

Respect for Context

Participating Members commit to using and sharing Covered

Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.

Data Minimization

De-Identification & Retention: Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes.

Data Security

Participating Members commit to implementing reasonable measures to protect Covered Information against unauthorized access or use.

Integrity & Access

Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to offering Owners and Registered Users reasonable means to review and correct Personal Subscription Information that they provide during the subscription or registration process for Vehicle Technologies and Services.

Accountability

Participating Members commit to taking reasonable steps to ensure that they and other entities that receive Covered Information adhere to the Principles.

These appear well founded and reasonable guidelines. However, it will not necessarily be the case that all users will be either owners or registered. In any event these guidelines will be superseded in all cases by legislative requirements under the GDPR where a conflict arises.

In that situation, activation of the vehicle should provide for an alert mechanism to the user that the vehicle is connected and relaying data to 3rd parties. How this alert occurs is flexible but again, the guiding principle must be one of informed, explicit and unambiguous consent. The use of a warning light on the dashboard may be compliant but only if there is sufficient universality to the warning light and general public understanding of the meaning of the warning light. An audio warning would also be a potential solution, however, language selection would also need to be built in. Other possible solutions may also be envisaged but one issue that needs to be considered in all of these potential solutions is whether consent is demonstrated by starting the vehicle or undertaking another step (for example pushing another button in the vehicle) which is more closely compliant with the provisions of the GDPR.

Moreover the addition of a consent mechanism separate to starting the vehicle might also help compliance with other provisions of the GDPR, particularly withdrawal of consent and the right to be forgotten. For example, if prior to starting the vehicle one had to slide a switch to the right to activate the connected element of the vehicle or to the left to deactivate the connection with the vehicle inoperative if the switch is not moved in either direction. On the other hand, legislation may mandate that vehicles have these safety devices and prohibit their de-activation.

In the US, the NHTSA in their 90 day rule making process for V2V communications indicated that mandatory safety devices would require higher levels of data protection than those which were voluntary. If so one would expect even stronger indices of consent to the use of connected devices, as well as strengthened use, storage, access and security obligations on the data controller.

9.1.3 9.1.3 Non-consensual data acquisition

By its very nature Cloud LSVA utilizes technology that potentially acquires personal data of 3rd parties without their consent, specifically other road users including cars, pedestrians etc.

Delizia Diaz, Legal Counsel and Data Protection Officer at Jaguar Land Rover, has said:

> Relying on consent as the sole legal justification for all data use cases would be extremely difficult and un-user friendly for autonomous vehicles. Other legal justifications for handling personal data are available and may, in certain circumstances be more adequate in an

autonomous vehicle environment. In our view, there needs to be some level of mandatory data sharing for autonomous vehicle infrastructures to operate.

This view reflects the reality that for autonomous or semi-autonomous vehicle technology to truly work mandatory data sharing is essential. What is unclear is whether the other legal justifications for handling data are fit for purpose in the context of Cloud LSVA. The two closest analogies for non-consensual acquisition of data are CCTV (closed circuit television) and drone photography. A quick analysis of both situations may prove instructive.

9.1.4 CCTV analogy

CCTV use requires justification as to purpose. Thus CCTV is relatively easily justified if the purpose is to provide security as distinct from monitoring the activities of employees. In Cloud LSVA the justification of human safety would presumably be a strong justification of the technology. However, although it does justify the non-consensual acquisition of data, it does not provide a blank cheque so to speak. The data collection must be proportionate so that the data collected is adequate, relevant and not excessive. Moreover it cannot be used to justify data acquisition of personal data where there might be an expectation of privacy by data subjects. Furthermore, the area which is the subject of CCTV recording should have appropriate and sufficient signage indicating that data acquisition is taking place. Finally, information should be available to ensure that data subjects or other individuals are in a position to contact the data controller (and processor) to access the data protection policy in operation with respect to the CCTV image recording.

For Cloud LSVA technology this provide one solution. Provided the only use to which the data is being acquired for is public safety this would justify the non-consensual acquisition of personal data provided it was coupled with the following:

Some indication that the vehicle is (a) recording images and (b) connected to the Cloud (for example, a coloured light on the vehicle which illuminates when the technology is in use)

Clear manufacturer marking on the vehicle (for example the company nameplate or logo).

This would then provide 3rd parties with knowledge that they are being recorded and the information is being stored remotely as well as the identity of the entity making the recording (the manufacturer) who could be contacted with respect to their data protection policy.

The justification of CCTV would require a Privacy Impact Assessment as well as the risk analysis vis-à-vis recording of non-consensual images to increase transportation safety.

The CCTV approach provides the best alternative route in non-consensual personal data acquisition. However, it might be useful to examine the second option relating to drone photography.

9.1.5 Drone videography and data protection

Where Cloud LSVA captures external personal data, for example vehicle registration plates, pedestrian faces etc., the general principle is that only that information absolutely necessary to achieve the objective of Cloud LSVA should be acquired. General acquisition of data may be justified in the same manner as that of CCTV cameras as set out above, but even then it may require anonymization of the data (eg pixelating of vehicle registration plates, blurring of faces) by analogy to the proposed treatment of drones. In particular, the Article 29 Data Protection Working Party 01673/15/EN Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones offers some guidance. In some instances, facial profiling of pedestrians may be necessary (for example, are they paying attention at a crosswalk) and this will pose further difficulties for the acquired data.

In V2V communications privacy by design remains crucial. In that regard, the NHTSA Notice of Proposed Rule on V2V Communications (49 CFR Part 571) is useful. It proposes that no information which would identify the vehicle (either VIN or license plate) or owner/driver should be contained in the V2V communication. Further discussion is in train to minimize privacy issues in V2V communications. This can be read in conjunction with ISO/TC204/WG16 known as 'ISO 24100 Intelligent transport systems – Basic principles for personal data protection in probe vehicle information services' which provides additional material.

These technologies permit the acquisition of large amounts of data without the knowledge never mind the consent, of the data subjects involved. Moreover the potential for misuse of the acquired data is higher due in particular to the bulk nature of the acquisition. It seems that CLOUD presents the same issues.

The June 2015 Opinion of the EU Working Party on Privacy and Data Protection Issues relating to Drones represents an up to date position of best practice which can be applied to the development stages within CLOUD. The main provisions of this Opinion can be summarised as follows:

- Suitable criteria for legitimate processing:
    - Purpose limitation: processed only to the extent necessary for the purposes
    - Data minimisation: non-essential data should not be acquired
    - Proportionality: to avoid the acquisition of unnecessary personal data
- Transparency:
    - Need to inform the data subjects of the data acquisition
- Security:
    - Protection of the data through anonymisation techniques
    - Cyber security particularly where the data is held on a cloud platform

Criteria for legitimate processing: for the CLOUD programme the issues of data minimisation and proportionality are crucial. Only that data necessary to achieve the CLOUD objective should be acquired

and that may require that CLOUD does not use the most technologically advanced equipment. For example, do the video recordings have to be of exceptionally high definition? Is it enough to be able to recognise that it was a truck and not a van in order to satisfy the purpose of CLOUD or would one need to be able to read the number plate of the van? The guiding principle should be: Just because I *can* does not mean I *should*. The equipment should be limited to what is necessary only.

Transparency: this is more contentious for CLOUD. How does one inform every individual that might possibly be the subject of data acquisition? In truth this is more likely to require specific legislation similar to that in CCTV operation and as recommended by the Working Group. However, in the meantime, one might consider thinking outside the box. In semi-autonomous truck development, the headlights change to a blue shade when the truck is on autopilot. Could some other visual sign be applied for CLOUD? More research from a legal point of view needs to be undertaken although it may be that responding to the issues of proportionality and security may minimise the importance of this particular issue.

Security:

Data anonymisation

One way of addressing transparency is to take steps to anonymise the data being acquired, which is also required to ensure the security of the information post-acquisition. The use of 'sufficiency' in data acquisition may provide some anonymisation, where for example the quality of the video recording is of insufficient quality to permit identification. In the absence of that, are there other ways of protecting the data subject: for example do the video recordings need to be identified by location? Is that crucial to the purpose for which the recording is to be used. A video recording of a data subject without any indication of the location would probably render it impossible to identify the data subject even if captured in high definition.

One issue of concern would be a solution which sought to anonymise the data after acquisition, say through blurring of facial details. CLOUD developers should not forget that the unaltered data on acquisition must comply with the rules as well.

Cyber security

There is a further distinct issue with security and that is the security of the data itself from unauthorised access. This is particularly important where the information is held in the cloud and may be hacked or otherwise breached. All stored information must be protected with the greatest possible level of protection from unauthorised breaches at all stages of development. This must be an integral element in the design and development process.

In many ways, a fuller analysis of these provisions presents as many difficulties as obtaining consent would. Anonymisation and pseudoanonymisation may not necessarily provide the relevant safeguards

required for data protection and in fact may simply put in an additional and expensive layer of quasi-protection that could be better achieved by the CCTV approach and strengthened protections in the access and storage of the acquired data.

Conclusion

Of course in the absence of specific regulatory provisions with respect to data acquisition for connected, autonomous and semi-autonomous vehicles any advice constitutes informed speculation only. Having said that, based on the analysis of a variety of primary sources, one is inclined to provide the following summary for the most likely best practice approach to the non-consensual acquisition of personal data in Cloud LSVA.

- Non-consensual acquisition of personal data would need to be justified by way of a risk assessment and Privacy Impact Assessment.
- The vehicle would have to signal to other road users and pedestrians that image recording was in operation
- The vehicle would have to have a clear manufacturer mark that would enable individuals to know who to contact
- A data protection policy would have to be in operation by the manufacturer and readily available upon request.

9.2 9.2 Data Controller and Processor

The GDPR essentially imposes similar liability on a data processor as currently exists on the data controller. In connected vehicles using Cloud LSVA technology the allocation of responsibility between controller and processor (and in certain situations one could be both a data controller and data processor) will need to be clearly defined within a contractual risk allocation framework.

9.3 Administration, Sanctions and Fines

Data protection policy will be made uniform through a “One Stop Shop” approach. Under this policy one of the national Data Protection Agencies will take the lead in any action for breach of these provisions with other national agencies acting in support. An overall co-ordination committee will attempt to create the uniformity in approach the failure of which in the previous provisions provided not only conceptual uncertainty but practical differential approaches at member state level.

The GDPR provides for fines up to €20 million or 4% of worldwide turnover in the event of a breach of data protection laws.

10 Recent case law

10.1 Cahen v Toyota Motor Corporation

Cahen v Toyota Motor Corporation is a case being brought by two Californian residents against Toyota and General Motors. It is part of a class action on behalf of other Californian residents. The two plaintiff purchased a 2008 Lexus RX400 and a 2010 Chevrolet Volt. The essence of their claim falls into two basic elements.

> First, that the connected cars collect personal information and share that information with 3rd parties by way of an unsecured transmission.
>
> Second that the connected cars are vulnerable to hacking rendering the vehicle open to being controlled by persons outside the vehicle.

In order to bring the case, the plaintiffs alleged they suffered harm from the misrepresentations of the manufacturers that the connected cars were safe and that had they been aware that this was not the case they would not have bought the cars. Only the first issue is of concern to Cloud LSVA and it is to this alleged invasion of privacy that we now turn.

Plaintiffs based their case on common law, Federal law and Californian constitutional law. However, they were unable to show any actual privacy breach arising from the transmission of the personal data. Instead they alleged potential future harm to their privacy rights which entitled them to a claim in economic damages, specifically the diminution in value between a data secure vehicle that they thought they had bought and the data insecure vehicle they actually received.

The court of first instance rejected their case based among other things on the fact that they even if they could establish that the transmission of data was not secure, they had not proven actual harm and could not rely on allegations of potential future harm. Indeed the judgment laid emphasis on the failure of the plaintiffs to demonstrate any real potential for the malicious or accidental release of sensitive information such as social security or credit card numbers. Essentially the court was indicating that although the information was personal in nature, it's release would not lead to the traditional concrete forms of loss that arise in other cases where say credit cards details may become publically available or where the release gives rise to identity theft as is the case where social security numbers are released.

In any event, the court went on to say that even if the court was wrong and at law there was liability for potential future harm, plaintiffs could not establish economic damage since all vehicles in the US sold

post 2008 would suffer from the same unsecure data transmission process and so all vehicles along with the plaintiffs would suffer a similar loss in value, thus there would be no specific loss to the plaintiffs.

The case is currently on appeal to the Federal Circuit court. Although it is clear that the litigants appear agenda driven, the application of the new provisions of the GDPR to a similar set of facts might give rise to a different outcome. Liability under the GDPR is for breach of data and not based on the harm which might arise from that breach. This is a regulatory infringement. The plaintiffs sought a harm based remedy, that is the payment of damages for a claimed loss. In reality such claims are not likely given that the likelihood of a breach of the data acquired under Cloud LSVA will not normally give rise to a privacy breach causing civil harm. But it is the breach itself which both the Directive and the GDPR imposes sanction on and it is that which must be guarded against.

11 International Data Transmission and Storage

Sharing data with external actors must be consistent with the needs for which the data was initially gathered. If such information is to be shared with entities within the EU then, as the parties are both subject to EU law and the data protections provided thereunder, such sharing is more easily undertaken.

However sharing information with entities outside of the EU poses more difficulties. The guiding principle is that the data acquired may only be transferred where it can be established that it will benefit from the same level of protection as it would within the EU.

There are two possibilities:

First the EU has certified that a number of jurisdictions have sufficient data protection rules which are the equivalent of that which operates in the EU. These are

- Norway, Liechtenstein and Iceland (EEA countries)
- Andorra
- Argentina
- Canada (commercial organisations),
- Faeroe Islands
- Guernsey
- Israel
- Isle of Man
- Jersey
- New Zealand
- Switzerland
- Uruguay
- US Department of Commerce's Safe Harbour Privacy Principles – now in re-negotiation following an ECJ court decision

Second, where the transfer is sought to a country other than one list above, it can only be undertaken where there is a contractual obligation on the external entity to manage the data in accordance with the same level of protection as arises under EU law. These contractual arrangements must use the EU Model Contract if one is to be certain that they are compliant with EU law. If the parties want to use their own contract they must get prior approval from the relevant data commissioner. This will involve submitting the proposed contractual provisions. This approach is certainly not recommended and it would be difficult to see why Cloud LSVA would depart from the Model Contract.

Finally issues may arise with respect to sharing information with state agencies for criminal justice purposes. It would be important that a protocol is put in place to deal with such requests.

The international nature of automobiles will give rise to jurisdictional issues as to where the data has been collected as well as where it is stored. The previous rule which allowed equivalency of data protection to permit dealing with EU data outside the EU remains even though Safe Harbour as a generic EU-US agreement was struck down by the EU courts. Its successor, Privacy Shield provides for continued data exchange based on organisations that have signed up to Privacy Shield principles. In any event the same affect can be achieved between the EU and other jurisdictions, including the US, through the use of standard contract provisions or binding corporate rules imposing such protections.
In 2018, an entity not established in the EU which either (a) offers goods or services within the EU or (b) monitors the behaviour of data subjects within the EU must nominate a representative within the EU to liaise with supervisory agencies and other stakeholders. Some aspects of Cloud LSVA may come within part (b).

12 Conclusion

In an ideal world, there would be a uniform internationally agreed regulatory framework that would prioritise safety over data protection. That is not nor is it likely to be the case for some time to come.

This new technology will involve both the consensual and non-consensual acquisition of personal data from data subjects and will in the short term (just over a year away) be governed by enhanced data protection provisions from the GDPR.

The net effect of this Regulation will be to place manufacturers using this technology in a legal position almost identical to that of Google and Facebook. Car manufacturers will in addition to making physical vehicles also become responsible for content and data management.

Further, other contributors to this technology, including contracted work to other IT service providers, across the supply chain to the ultimate vehicle will likely be exposed to liability based on being either data processors or data controllers.

The only way of managing this liability risk in data management is to ensure processes conform with the over-arching provisions of the GDPR from acquisition to destruction. At each stage of the development

of the technology, the privacy impact consideration needs to be addressed. Just because the technology can do something does not mean that it will be allowed to do so. Best efforts should be made to ensure regulatory compliance with existing laws no matter how difficult. If the technology cannot be made compliant but is essential to the proper functioning of the vehicle safety feature, consideration should be given as to how risk and liability allocation can be managed using contractual provisions. The existence of international standards of best practice in this area will also be of assistance. General ISO standards in the ISO 27000 designation, such as in particular ISO ISO 27001 (Information Security Management System) and ISO 27032 (Guidelines for Cybersecurity) will provide some guidance with respect to these obligations but the fast moving nature of the technology will maintain the challenges discussed in this paper.