Agenda

• The hard shoulder: European regulation
  Andrew Bulley Partner, EMEA Centre for Regulatory Strategy
• The cyber risk factor: how exposed is the motor insurance industry?
  Jacky Fox Director, Cyber Risk
• Indicating right for GDPR: Personal data and regulation
  Donal Murray Director, Audit and Assurance
• Where will the future of mobility take us?
  Justine Bornstein Insight lead and programme manager for the UK Future of Mobility Practice
• Slow or fast lane? Irish motor insurance trends;
  Darren Shaughnessy - Senior Manager, Audit and Assurance
• Panel Q&A hosted by Ciara Regan Partner, Audit and Assurance
EMEA insurance regulation and the motor industry
Andrew Bulley | Partner | EMEA Centre for Regulatory Strategy
Centre for Regulatory Strategy, EMEA
Providing a forward-looking view of the most important regulatory developments affecting financial services firms

The new regulatory landscape – our response

- **Thought leadership**: advise on regulatory change, with focus on the strategic, business model and aggregate impact

- **Horizon scanning**: monitors and analyses key emerging regulatory developments

- **Global collaboration**: local representation across Europe and leads the Global Centre for Regulatory Strategy with Deloitte counterparts in the Americas and Asia-Pacific

The work of the Centre

- Develop insights, blogs, publications and presentations

- Advise on the aggregate impact of relevant forthcoming regulatory developments

- Maintain active cross-EU dialogue with the ECB and the ESAs

The Centre is led by **David Strachan**, who joined Deloitte from the FSA where he was Director of Financial Stability, and **Andrew Bulley**, who joined Deloitte from the PRA where he was Director of Life Insurance Supervision
Global outlook
Looking ahead to 2018

Major drivers of regulatory agenda for 2018

• Waning global consensus
• Major areas of unfinished business remain
• Key leadership changes in international bodies

Supervisory expectations

• Political and economic climate
• Risk appetite and stress testing

Near-term challenges

• Business model pressure
• Price bubbles and consumer indebtedness

Longer-term challenges

• Innovation, ageing populations, and climate change
• Impact on business models and risk profile
EMEA Regulatory Outlook 2018
The top seven thematic issues of strategic significance across financial services sectors and a number of sector-specific issues

1. Meeting multiple regulatory deadlines
2. Preparing for Brexit
3. Supervisory spotlight on business models: the challenge of low interest rates
4. Data protection, innovation and good customer outcomes
5. Customer vulnerability and cross-subsidies – broadening the perspective
6. Cyber risk and resilience
7. Managing risks from internal models
Insurance regulation in 2018
Overview of insurance sector-specific issues

**Continuing regulatory and capital change**
2018 will be dominated by discussions about future changes rather than implementation.

**Profitability and low interest rates**
Conduct will be placed in sharp focus.

**Profitability and soft markets**
Profitability will remain squeezed and underwriting standards and policy term limitations could deteriorate.

**Disruption and innovation**
Pricing practices will come into regulatory focus.
Motor insurance key themes

- Low interest rates
- Vulnerability
- European Regulation
Motor insurance
UK motor market overview – Association of British Insurers

£194m underwriting loss
The £194m underwriting loss in 2016 was a significant decrease from the £33m underwriting profit in 2015, the first time that the UK motor insurance market made a profit since 1994.

£33.3m paid per day
Insurers paid out £33.3m per day in motor claims of which £23.6m was for domestic claims and £9.7m related to commercial claims.

£485 average premium
By Q3 2017 the average motor premium for private motor had risen to £485, following the rise in IPT from 10% to 12%, as well as the Ogden discount rate change from 2.5% to 0.75%.

98.4% claims acceptance
In private motor, 98.4% of the total number of claims made in 2015/16 were accepted.

£9,924 average Bodily Injury claim
Whilst average claims for bodily injury are high, the overall average for all types of private car claims was £2,839.

“The ABI’s Premium Tracker - the only market survey which measures prices consumers actually pay for their motor cover, rather than quotes - shows that in the fourth quarter of 2017:

• The average price paid for private comprehensive motor insurance was £493. This was the highest quarterly figure since ABI started collecting the data in 2012, up 6% on the same quarter 2016.
• The average premium paid over the whole of 2017 at £481 was 9% higher than the previous year, and the highest since ABI started collecting this data back in 2012. This added an extra £40 to the average premium.
• The average cost of motor cover has leapt by 29% since 2014.”

Source: Association of British Insurers,
Low interest rates
Insurance
Profitability and low interest rates

• **Insurers**: moving further into alternative and higher risk investment classes
• **Supervisors**: strengthening challenge on board and senior management understanding of the implications for risk profile and capital strength
• **Conduct**: sharp focus on risk of consumer detriment in pursuit of profitability, particularly for vulnerable consumers
• **Ogden rate**: used to value periodic payment orders (PPOs), reduced from 2.5% to -0.75% in February 2017. Subsequent consultation on updated approach that would increase rate
• **2018 EIOPA stress test**: low interest rates and potentially impact of rising interest rates

Insurance
Profitability and soft markets

• **Soft market**: supply of insurance risk capital is unlikely to dry up in the near term
• **Financial resilience**: UK Firms should expect scrutiny of contingency planning, catastrophe modelling and stress testing
• **Supervisors**: concerned by the adequacy of rates and reserving, softening policy terms and allowance for the impact of extreme events
• **Cyber underwriting risk**: area of special focus
• **Resolution planning**: expect to remain within the framework of national regulation in 2018

A prolonged hardening of the market creates a double-edged risk for supervisors – on the one side, long-running depressed profitability coupled with a deterioration in underwriting standards and policy terms and on the other, the risk of disruption in a turning market.
Conduct themes for 2018 and beyond
Vulnerability & cross subsidies

Shift in supervisory strategy to prioritise the needs of the most vulnerable and least resilient consumers.

Ongoing attention to the potential for cross-subsidisation to lead to consumer detriment.

Focus on legacy and back book customers who may be vulnerable and less likely to switch to new, better value, products and services.

The FCA is starting to look at the treatment of vulnerable consumers in specific markets.

Firms with complex supply chains and distribution arrangements may struggle to identify and safeguard vulnerable consumers.

Data

Concerns that Big Data may lead to increased risk segmentation, higher prices for some consumer groups, and increasing use of non-risk pricing (price discrimination).

Increasing regulatory scrutiny of the use of data in underwriting and pricing, in particular price optimisation/discrimination and cross-selling.

GDPR: the Financial Ombudsmen Service has predicted that the use of customer data could be the next cause of large numbers of consumer complaints.

What is the FCA looking at in insurance more generally?
The FCA and Motor insurance

Market study looking at the sale of general insurance add-ons. Guaranteed Asset Protection (GAP) insurance new rules:
- Confirm that they want the product following sale of primary product
- Ban pre-ticked boxes
- Publish claims ratios

FCA research on how motor insurers and intermediaries disclosed their fees and charges to customers. FCA found that:
- Some firms did not clearly disclose the fees and charges as required
- Some firms charged unreasonably large fees or punitive exit fees

New rules about insurance renewals for retail consumers:
- Disclose last year’s premium at each renewal
- Encourage consumers to check their cover and shop around
- Additional prompts for consumers who have renewed four or more consecutive times
The FCA is currently undertaking two insurance-related market reviews

- End-to-end relationships in insurance distribution chains
- Competition in the wholesale insurance broker market
European Insurance Regulation

EIOPA’s objectives

**EIOPA’s objectives:**

- Contribute to a **sound, effective and consistent** level of regulation and supervision
- Ensuring the **integrity, transparency, efficiency and orderly functioning** of financial markets
- Strengthening international **supervisory coordination**
- Preventing **regulatory arbitrage**
- Ensuring the **taking of risks** is appropriately regulated and supervised
- Enhancing **customer protection**

**EIOPA’s tools to fulfil these objectives:**

- Issuing **guidelines and recommendations**
- Taking individual **decisions addressed to competent authorities or individual institutions** in specific cases
- Developing draft **regulatory technical standards** and draft **implementing technical standards** in specific cases
- **Issuing opinions**
- Developing **common methodologies** to assess the effect of product characteristics and distribution processes on the financial position of institutions and consumer protection
- Collecting **information** concerning financial institutions
- Providing a centrally accessible **database** of registered financial institutions

“The objective of the Authority shall be to protect the public interest by contributing to the short, medium and long-term stability and effectiveness of the financial system, for the Union economy, its citizens and businesses.” - EIOPA Regulation, Article 1
European Insurance Regulation
EIOPA’s approach to conduct of business

Consumer trends reports
Snapshot of existing and emerging cases of consumer through quantitative and qualitative information

Market monitoring
Scrutinising new and existing financial activities to identify trends, potential risks and vulnerabilities that may lead to consumer detriment

Retail risk indicators
Pre-emptively assess how product characteristics and distribution processes can affect customers

How is EIOPA tackling conduct issues?
- Conduct framework tools
- Key Information Documents
- Insurance Distribution Directive

Thematic reviews
Investigate in depth specific activities or products that may cause consumer detriment
<table>
<thead>
<tr>
<th>InsurTech</th>
<th>IDD and PRIIPs</th>
<th>Conduct and culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>• New <strong>cross-cutting theme</strong> to EIOPA’s objectives</td>
<td>• Implementation of the <strong>IDD</strong></td>
<td>• <strong>Conduct of business oversight cultural visits</strong> in 2018/2019</td>
</tr>
<tr>
<td>• Thematic review of the insurance industry’s <strong>use of Big Data</strong></td>
<td>• Production of documents related to and required by <strong>PRIIPs</strong></td>
<td>• Develop and report on <strong>retail risk indicators</strong></td>
</tr>
<tr>
<td>• <strong>Cyber risk</strong></td>
<td>• Shift to <strong>monitoring consistent implementation</strong> and ensuring supervisory</td>
<td>• Analysis of <strong>conduct risk throughout the product lifecycle</strong></td>
</tr>
<tr>
<td>• Promote <strong>supervisory convergence</strong>, facilitate a <strong>level playing field</strong> and pursue a <strong>technology-neutral approach to financial innovation</strong></td>
<td>• Contribute to a <strong>review of the PRIIPs regulation</strong></td>
<td>• Potential <strong>thematic review</strong>, which may involve consumer testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Annual trends report</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assessment of products that <strong>place risk with consumers</strong></td>
</tr>
</tbody>
</table>
Automotive Hacking and vehicle autonomy

Insurance implications?

Jacky Fox – Cyber Lead Deloitte Ireland
“Car companies are finally realising that what they sell is just a big computer you sit in.” — Kevin Tighe (senior systems engineer at the security testing firm Bugcrowd)
Autonomous cars
Modern cars have millions of lines of code
Cyber Security is a recent introduction for automobiles
Autonomous car numbers are forecast to rise
Are we advancing car technology faster than we can secure it? (think IOT attacks)
There are banks of statistical data for actuaries to estimate and quantify the risk, likelihood and impact of human controlled vehicle accidents
There is an addition of many more parties to an accident with autonomy – developers, 3D map providers, how can you apportion blame?

Source: BI Intelligence Estimates, 2017
## Autonomous cars
### Levels of autonomy

<table>
<thead>
<tr>
<th>Level</th>
<th>Autonomy</th>
<th>Driver Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No automation</td>
<td>Driving as we know it. The human driver controls the brakes, accelerator, steering and gears.</td>
</tr>
<tr>
<td>1</td>
<td>Driver assistance</td>
<td>Majority of functions are controlled by the human driver, however there is a specific function (steering or speed) that can be done by system.</td>
</tr>
<tr>
<td>2</td>
<td>Partial automation</td>
<td>The driver can disengage both hands and feet from controlling the vehicle (lane centering and cruise control engaged).</td>
</tr>
<tr>
<td>3</td>
<td>Conditional automation</td>
<td>The system can shift all “safety-critical functions” to the vehicle.</td>
</tr>
<tr>
<td>4</td>
<td>High automation</td>
<td>Can perform all safety-critical driving functions and monitor roadway conditions for an entire trip.</td>
</tr>
<tr>
<td>5</td>
<td>Full automation</td>
<td>The system performs at least equal to that of a human in all scenarios, over all terrains (dirt roads, grass and others).</td>
</tr>
</tbody>
</table>
Future of automobiles
Autonomy leads the way

**Ford’s head of product development: autonomous vehicle on the market by 2020**

Raj Nair, Ford’s head of product development, expects that autonomous vehicles of SAE level 4 (which means that the car needs no driver but may not be capable of driving everywhere) will hit the market by 2020.
*(Source: autonews)*

**BMW to launch autonomous iNext in 2021**

At their annual shareholder meeting, BMW CEO Harald Krueger said that BMW will launch a self-driving electric vehicle, the BMW iNext, in 2021.
*(Source: Elektrek)*

**Ford CEO announces fully autonomous vehicles for mobility services by 2021**

Mark Fields, Ford’s CEO announced that the company plans to offer fully self-driving vehicles by 2021. The vehicles, which will come without steering wheel and pedals, will be targeted to fleets which provide autonomous mobility services. Fields expects that it will take several years longer until Ford will sell autonomous vehicles to the public.
*(Source: Reuters)*
Autonomous cars
Exploiting self driving cars

**Connected Car**

Autonomous cars are more likely to have a stable internet connection (always connected) and that can provide opportunity to attack remotely.

**Multiple threat vectors**

Much focus of “car hacking” can be on the car itself, but when an attacker knows what sensors are being used, why not trick the sensors?

**Don’t hack the car, hack the world it sees**

By altering just 4% of an image, a Google paper showed that AI could be fooled into perceiving a different object 97% of the time. 3D mapping and Lidar have many challenges to correctly identify both static and dynamic objects and data feeds.

**Artificial intelligence**

Would your car kill the dog or the crawling child?
Remote access threat

- A Connected car exponentially increases the possibility of remote attacks as it becomes just another computer online.

- Any internet facing app that is not directly on the CANbus, could still communicate with it.

- CANbus accepts all messages, there is limited security in place. Like the internet it’s functionality has been extended.

- Sub-par cyber security on apps has provided attackers with remote access to vehicles in the past.

Potential ransomware attacks

One morning, in the not-too-distant future, you're in a rush to go to work — but when you put the keys in the ignition, your car does not start.

Instead, a message flashes on the dashboard screen: You've been hacked. Pay the hacker €5,000 in bitcoin within 24 hours, or you're locked out of your vehicle permanently.
Automotive hacking
What has been hacked?

- Engine
- Brakes
- Sensors
- Dash Displays
- Acceleration
- Steering
- Central Lock
- Power Seats
- Windows
- Lights
- Wipers
- A/C
- Radio Control
- Comms
- GPS
Cyber Security researchers were able to hack into a Chrysler Jeep as it drove down a highway at high speed in 2015. All from the comfort of their home, ten miles away.

- Controlled window wipers/ wiper fluid
- Air conditioning
- Radio and disabled control knobs
- Killed the engine
Automotive hacking
Live attack

**How was this executed?**

- A laptop was linked up to a smart phone to get access to the US Sprint network
- The hacker scanned for vulnerable car IP addresses
- A chip was exploited that contained six lines of code
- The car control software was reprogrammed over-the-air with custom malware
- Remote CAN messages were sent to control car features

**What was the response?**

- A recall of more than 1.4 million cars and trucks
- Campaign to ensure customer safety

**How could this impact insurance?**

- What if the breaking or steering system had been attacked?
- How would an insurer attribute any damage or loss of life that occurred? Who’s at fault?
  - The hacker
  - The software developers
  - The car testers
  - The manufacturer
  - The “driver”
Limit connectivity to reduce risk

John Krafcik, the CEO of Alphabet’s self-driving car company WAYMO, announced that its vehicles will not have a consistent internet connection. Instead, they will periodically connect, exchange data then disconnect.

Learn lessons from history

Avoid IoT scenarios such as the broadcasting babycams and the attack of the vending machines.

Get the basics right such as malware attack detection and prevention measures, automate software updates and user awareness.

Installing a great new radio could be introducing more than nice sounds to your vehicle.

Hackers to the rescue – bug bounties

Tesla have put $10,000 on the table for any hacker that comes forward with a hack for its Model S car. Tesla is known to have cyber security as one of, if not their main safety concerns.
Car designers have to get security right all of the time to protect us, hackers only need one error to get in.

Automakers are good at making cars – this is a whole new ball game.

Have we learned from IoT security (or lack thereof) mistakes?

How will the auto industry cope with privacy concerns, location, recording etc.

Are the regulators ahead of development?

Existing insurance risk models will need a complete re-think, are you ready?

The 30 year old CANbus needs better encryption, device authentication and layered security.
The General Data Protection Regulation (GDPR) – Motor Insurance Impact
Overview
March 18
The General Data Protection Regulation (GDPR)

What is the GDPR?

In 1995, the European Union released the European directive 95/46/CE relative to personal data protection. Unlike regulations, directives should be transposed into national to be applicable.

On 4 May 2016, the EU Regulation on Data Protection (GDPR) has been published in the Official Journal of the European Union. The GDPR has entered into force on 24 May 2016 and will replace the former 1995 EU Data Protection Directive and create a unified data protection law.

The General Data Protection Regulation will apply as from 25 May 2018 directly across all 28 EU Member States after a two years implementation period. Under the new Regulation, Data Protection Authorities (DPAs) have investigative, corrective, advisory and authorization powers. They are entitled to impose administrative fines ranging from 2 to 4% of the groups worldwide annual turnover of the preceding financial year or EUR 10 to 20 million, whichever is higher for infringements of data subject rights, non-compliance with an order of the DPA or the obligations of the controller and processor.

The Charter of Fundamental Rights of the European Union became legally binding across the EU with the entry into force of the Treaty of Lisbon on 1st December 2009 introducing the “Protection of personal data” as a fundamental freedom (art. 8)
Core GDPR Principles

Stronger Data Subject Rights

Right not to be Profiled

Only allowed:
• If necessary for the performance of a contract
• If authorised by law
• If based on the data subjects explicit consent

Right to Data Portability

• Right to receive personal data in a structured and commonly used and machine-readable format
• Transmit to another data controller directly where technically feasible

Key Challenges

• Interoperability of systems and identification of data – when an objection is submitted. Organisations must have the technical measures to fulfil this throughout all systems where analytics is carried out

• Organisations will be expected to transfer an individuals personal data to another service provider upon request if they have the technical means – this other service provider may be a competitor
Data Portability

What is the scope?
The GDPR is clear that portability relates to data which he or she has provided to a service provider.

Diagram:
- Data Subject
  - Application
  - Servicing Comms
  - Claims
  - Telematics

Data Controller

Raw Data

Data Controller (competitor)

Raw data not information!
Stronger Data Subject Rights
Core GDPR Principles

Right to be Forgotten (Erasure)
- Requests must be actioned without undue delay
- If data was made public, inform concerned third parties
- Limited to specific grounds and not absolute and can be refused on a number of grounds including where processing is necessary for public health reasons, scientific research as part of a legal obligation or legal defense
- Requests must be actioned without undue delay – the turnaround time under GDPR is one month (previously 40 days)

Right to Access
- Requests must be actioned without undue delay
- The fee has been abolished

Are Data Subject Rights a business enabler?

Key Challenges
- Interoperability of systems and identification of data – when a request for rectification, erasure or access is made, do organisations have the technical measures to fulfil this throughout all systems where the personal data is stored
- Not having clear data owners who can manage and fulfill requests leaves an organisation open to risk
- The abolishment of the subject access request fee leaves organisations open to frivolous requests
Core GDPR Principles - **Consent**

Consent to collect personal data must be freely given, specific and in some cases explicit. The consent must be gained prior to collection of the personal data and must be distinguishable and clear. The burden of proof is on the organisation as the data controller and the data subject has the right to withdraw consent at any time.

**Key Challenges:**
- The collection of special categories of personal data (sensitive personal data) can only occur if consent is received OR if the organisation can prove the processing of that data relates to certain processing buckets......
Privacy by Design and by Default and Privacy Impact Assessments

Core GDPR Principles

**Privacy by Design** is not a new concept but it is now a requirement under GDPR. Essentially, what it means is that privacy implications are considered at the start or re-design of any IT system, new product or service, software development, process change that involves personal data. The lifecycle of the personal data must be accounted for at all times through privacy enhancing controls using data lifecycles and data inventories as living documents. The aim is to be proactive instead of reactive and embed privacy into business operations.

**Privacy by Default** promotes that an organisation's modus operandi is to automatically apply the strictest privacy settings to any new product or service. In other words, a consumer does not have to adjust any privacy settings as they are already automatically set to the most secure.

**Privacy Impact Assessments** must be carried out on any new project that involves the processing of personal data that is likely to be a high risk to the rights and freedoms of individuals. DPO's must be consulted and if the PIA identifies a high risk, the supervisory authorities must be notified and consulted prior to the processing.

Key Challenges

- The biggest area that organisations struggle with is putting a solid privacy framework in place. To be able to comply with Privacy by Design elements, the creation of data lifecycles and data inventories are key.
- Data minimisation through only collecting what is necessary and anonymising or pseudonymising data set.
- Considerations relating to the redesign of health devices as well as the cloud environment that they may dump data to.
Deloitte Survey Results Snapshot

ONLY 15% expect to be fully compliant

61% of respondents see further benefits of remediation activities beyond compliance, supporting Deloitte's view that the GDPR offers the ideal opportunity to view privacy as a business enabler.

62% opting for a defensible position

1. Consent - ensuring consent is informed, unambiguous and recorded
2. Right to erasure - managing and facilitating data subjects' right to request the deletion of personal data
3. Records of processing activities - developing and maintaining a register of personal data processing
4. Accountability - keeping records of decisions and positions, and demonstrating compliance
5. Data portability - providing the ability to port personal data from one data controller to another in certain circumstances

40% of respondents are considering tools that will enable data flow mapping

A quarter of respondents have yet to decide how to approach compliance with Article 30, but the majority (57%) plan to undertake a manual data discovery exercise.

54% of respondents noted that the potential for large fines under the GDPR made a difference to their approach

64% of respondents are yet to prepare estimations on how many requests for erasure they are likely to receive.

59% of respondents have yet to prepare estimates on how many requests for data portability they are likely to receive.

57% of respondents have yet to decide how to ensure their consent mechanisms are compliant with the GDPR.

19% of respondents plan to undertake a re-consenting exercise.
Justine Bornstein, Insight lead and programme manager for the UK Future of Mobility Practice
What will the new ecosystem look like and how will it operate?

Meet Ben…

- he is a millennial living just outside the city
- he wants to pick up groceries
- he is ready to go home after a long day at work

Let’s explore his journey home
There are two profoundly different visions about how the future could evolve

**Insider view**

The industry will **evolve naturally** and **incrementally** toward a future mobility system that **retains its roots** in what exists today.

The key players, major assets, and overall structure of the **current ecosystem can remain intact** while change progresses in an **orderly, linear fashion**.

The incumbent mindset appears **dually focused** on sustaining the current model while **testing change in small ways**.

**Disrupter view**

A **whole new age** is dawning featuring **fully autonomous** cars accessible on demand.

Before long, a **tipping point** will occur, after which the **momentum of change will become unstoppable**.

**New entrants**, notably Google and Uber among others, are **catalysts** for transformation.

Unlike the stakeholders in today’s system, they **do not have vested stakes** to protect.

Source: Deloitte analysis, based on publicly available information and company websites
There are a number of forces that will influence the rate at which the new mobility ecosystem takes shape:

- **Regulation & Government**: Federal, state and local policies
- **Public Attitudes**: Human-machine interface, safety, shared economy
- **Technology Development**: Early experiments, pilot programs
- **Privacy and Security**: Cyber-security, communication protocols
- **Financial Valuations**: Technology investments, cost of capital projections
- **Employment Changes**: Dislocation effects, reactions, job retraining

Source: Deloitte analysis, based on publicly available information.
Disruption is coming...how will it impact sector revenues?

UK extended mobility ecosystem revenues

- **Automotive**: £249bn
- **Finance**: £37bn
- **Transportation**: £90bn
- **Technology**: £5bn
- **Media**: £4bn
- **Medical & Legal**: £8bn
- **Public sector**: £55bn
- **Energy**: £37bn
- **Insurance**: £14bn

~£500bn

Data from 2014-2015

Sources: Deloitte analysis, with data from Office of National Statistics, TechUK, Finance and Leasing Association, Legal Services Board, Department of Communities and Local Government, SMMT, Department for Transport, Magnetic, Statista.
Insurance coverage types

**Traditional coverage**

- **Comprehensive**: Protection for the policyholder’s vehicle for damages that are not related to a collision (e.g. natural disasters, falling objects, vandalism, theft).
- **Collision**: Protection for the policyholder’s vehicle for damages arising from a collision. Examples of covered incidents include hitting another car or hitting a stationary object.
- **Driver liability**: Protection for the driver against the damages caused to another person’s body (bodily injury liability) or property (property damage liability) because of the negligent operation of the vehicle.
- **Product liability**: Protection for OEMs and suppliers against component failure.
- **Other coverages**: Other traditional automobile insurance coverages include medical payments, under–insured/un–insured, and personal injury protection, among others.

**New coverage**

- **Product liability for autonomous vehicles**: In the future, the entities responsible for designing, building, and maintaining the hardware and software comprising an autonomous vehicle operating system may seek protection against catastrophic losses resulting from some or all of these components malfunctioning, resulting in a loss.
Premium need by coverage type

Note: Premium estimates do not account for the effect of self-insurance by large commercial fleets or vehicle manufacturers.
A new mobility ecosystem will emerge delivering seamless intermodal transportation faster, cheaper, and safer than today.

Source: Deloitte analysis
Value in this new ecosystem will be derived from consumer-centric data, systems, and services-oriented business models.

Future Mobility Value System

- **Experience Enablers**
  - Content creation
  - In-vehicle services
  - Predictive Content Analytics
  - Marketing & Advertising

- **Mobility Management**
  - Relationship Management
  - Predictive Analytics
  - Data Collection

- **Infrastructure Enablers**
  - Security provider
  - Operating system providers
  - Connected car technology

- **Physical Vehicle Development and Manufacturing**
  - Autonomous technology hardware suppliers
  - Car and Pod manufacturers and parts suppliers

- **Opportunity Space**
  - Digital and physical infrastructure
  - Fuel / energy providers
  - Roadways

These four fundamental areas of value creation manifest themselves in the new mobility ecosystem.

Source: Deloitte analysis
Automotive Value Chain 2025+ study approach
A multitude of different scenarios across time/markets/segments

Hardware platform provider
- Cars are **software based high-tech** products with OEMs providing the shell
- **Tech players** manage in-vehicle services and platforms

Suppliers and outsiders set the rules

Data & mobility manager
- **OEMs dominate** the automotive value chain through gated platforms
- OEMs set standards for **connected services** and **modern life infrastructure**

OEMs dominate the automotive world

The fallen giant
- The **technology hype cools down**
- Industry **outsiders like Uber enter the market** and provide affordable mass mobility
- Strong **displacement competition**

Stagnant car maker
- The automotive value chain remains mostly unchanged
- Hype around connectivity technologies is gone – cars are mere **vehicles for transportation**

Below technological possibilities

To the full extent
Vehicle automation

Half of respondents are not willing to pay for self-drive. The other half are willing to pay a high amount – due to younger generations being willing to pay more.

Willingness to pay for vehicle technology type

<table>
<thead>
<tr>
<th>Technology Type</th>
<th>2014</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full/partial self-drive</td>
<td>£677</td>
<td>£375</td>
</tr>
<tr>
<td>Alternative drivetrain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cockpit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Average expected price by automation has declined.

Consumers rate connectivity features (diagnoses and sends maintenance notifications) highly, but then they are not willing to pay for it – they expect it to come as standard.

People are more willing to pay for safety features.

The younger the generation, the more people are willing to pay for vehicle technologies.


Sample sizes – [2016: Pre/boomers, N= 544; Gen X, N= 253; Gen Y/Z, N= 451]
We fear our cars being hacked but we’re willing to share our data for a benefit...

Consumer opinion on personal data sharing and privacy

Benefits

I would share my personal information if I get significant benefits from it.  
68%

Risks

I would share my personal information with commercial third parties if I get significant benefits from it.  
51%

With my car connected to the outside world, I fear someone hacking into my car and risking my personal safety.  
63%

I believe personal data generated from my car is safe and secure from hackers.  
44%

I would share my personal information with anyone as long as I know what I am sharing and am comfortable sharing it.  
57%

Note: Percentage of respondents who strongly agreed or agreed have been added together.

Sample size – [N= 1,089]
Deloitte, a partnership established under the laws of Ireland, is the Ireland member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. Please see About Deloitte to learn more about our global network of member firms.

At Deloitte, we make an impact that matters for our clients, our people, our profession, and in the wider society by delivering the solutions and insights they need to address their most complex business challenges. As the largest global professional services and consulting network, with approximately 263,900 professionals in more than 150 countries, we bring world-class capabilities and high-quality services to our clients. In Ireland, Deloitte has nearly 3,000 people providing audit, tax, consulting, and corporate finance services to public and private clients spanning multiple industries. Our people have the leadership capabilities, experience and insight to collaborate with clients so they can move forward with confidence.

This communication contains general information only, and none of Deloitte, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018 Deloitte. All rights reserved