Executive Brief

Responsibility for Vehicle Security and Driver Privacy in the Age of the Connected Car

Sponsored by: Veracode

Duncan Brown
February 2016

IDC OPINION

The Connected Car is one of the primary use cases for the Internet of Things (IoT). Yet it is one of the least well understood in terms of cybersecurity. Recent media coverage has exposed critical vulnerabilities to the software that improves performance of the vehicle and the experience of the driver. Similarly, personal data may be collected from cars – for legitimate purposes – that could compromise the privacy of drivers. Veracode commissioned this study to explore how manufacturers are addressing these issues and to understand whether drivers are concerned about them.

Introduction

The prospect of allowing performance and entertainment functionality to be downloaded and upgraded directly to a car via the Internet is both exciting and terrifying. The ability for drivers to download software to navigate, park, communicate, conserve fuel, self-park, or other driver enhancements will revolutionize the automotive sector. Yet exposing a car to the Internet makes it vulnerable to cyberattack or malfunction due to glitches caused by poorly written software – either of which could render the car unstable or dangerous. Examples exist today in the form of widely published research, such as the demonstration in 2015 in which a Jeep Cherokee was totally taken over by a third party while driving at more than 110 km/h on a US freeway.

The implications of a connected car are vast, cutting across the interests of consumers, manufacturers, government safety regulators, and law enforcement. For vehicle manufacturers, the issues go beyond automotive design and safety to determining what impact becoming a software and application provider will have for their overall business. While manufacturers have been dabbling in embedded software systems design for some time, building an application development team able to compete with the likes of Apple or Google is a significant challenge. Doing it under the microscope of government regulated safety standards and liability concerns is another.

While IDC projects the total market for automotive-related IoT in 2016 is worth $140.3 billion, what portion will go to vehicle manufacturers, component manufacturers, and independent software vendors (ISVs) is not clear. The pressure is on, as already Apple and Google are producing in-car software platforms to allow access to smartphone applications from infotainment systems and are rapidly developing self-driving automotive prototypes – a move that would make them car manufacturers as well. It's not just the big guys, many ISVs have recognized the market potential and have already jumped in. Samsung, TomTom, and Verizon, for example, offer in-car applications.

The stakes for traditional automotive manufacturers are high: they are fighting for control, not only over the software business, but also their leadership roles in their own industry.

In this Executive Brief, sponsored by Veracode, IDC explores these issues and the current thinking within the automotive industry — represented by manufacturers, component suppliers, and industry bodies — to detect any variance between how manufacturers are preparing for the connected car in all its forms, and the expectations, demands, and concerns of the drivers. IDC conducted in-depth interviews with leading vehicle manufacturers and automotive industry representatives, as well as 1072 drivers across the UK and Germany, to shed light on:

- What are the cybersecurity implications of the connected car?
- Who is responsible for ensuring the applications are secure?
- Where does product liability lie with regard to the connected car?
- What are the issues and approaches for personal data and privacy?
- What types of applications that are drivers demanding?

Cybersecurity and Vehicle Safety

While automotive manufacturers are well aware of the issues relating to physical security for the connected car and liability thereof, the cybersecurity issues are less understood. This is new technology and the strategies for addressing these issues are still being formulated.

The prevailing approach by manufacturers is to keep separate the two cyber systems within the connected car — performance harness and infotainment harness — to limit "contamination" from the driver-accessible software leaking into the part that controls engine performance, braking and steering. Further, the performance harness would not be connected to the Internet, forcing software updates to be controlled during dealership visits. However, pioneering connected car manufacturer, Tesla, allows Internet updates to the performance harness with no user intervention. At the rate at which software needs updating across our smartphones and computers, it seems impractical to hold updates until the next maintenance visit, which could be every 6-12 months or even longer.

This might change, however, and rather soon. In 2018, EU legislation will require all new cars to be equipped with the e-call solution (essentially a subset of the concierge services being offered by some manufacturers such as GM's On-Star System), allowing a car to automatically contact the emergency services should it be involved in an accident. The impact of this regulation means that all cars will, by default, have a built-in SIM card to provide the required connectivity.

Based on our conversations with manufacturers, this represents an attractive, cellular-based communications path to update key vehicle software via a manufacturer-controlled gateway, still avoiding the Internet. It could also allow the car to be proactive in alerting the manufacturer to the development of a software vulnerability and the manufacturer to either remotely send a patch or alert the driver to the appropriate course of action.

While the industry is just beginning to debate cybersecurity issues surrounding connected cars, manufacturers interviewed for this research told IDC that it will be one to three years before connected car systems are implemented with full consideration of such concerns. The question for manufacturers is whether this is realistically feasible given the challenges ahead and the rate at which applications are being developed today.

Moreover, manufacturers need to consider the demands and concerns from their customers. Our research shows that around three quarters of drivers are slightly, somewhat or even very concerned about the safety of connected vehicles, as we will discuss in more detail shortly. Taking these numbers into account, a significant number of drivers might be reluctant to buy and use connected services due to their safety concerns. Manufacturers therefore really need to speed up their thinking, strategies, and implementations so as not to miss out on big opportunities.

Dashboard and Smartphone Connectivity

At the time of writing, there are two main concepts for what a connected car is: delivery of enhanced functionality and utility for a physical driver, and a completely autonomous car in which the driver is little more than a passenger. Innovations are occurring across both concepts, each with significant market potential. In each case, software – applications in particular – are the driving force behind this revolution in how we interact with our vehicles. Where software goes, independent software vendors (ISVs) are sure to follow, and to lead in innovation.

One particular area where this can clearly be seen is the flurry of activity around developing platforms that enable smartphones to tie directly to a connected car's infotainment system. Once viewed as high-margin, differentiating features amongst rival manufacturers, Apple (CarPlay), Google (Android Auto), and the Car Connectivity Consortium (MirrorLink) have developed their own solutions. The speed at which these companies are able to push out new solutions, functionality and continuous updates to their software is far beyond the capabilities of most manufacturers.

While manufacturers such as Ford (SmartDeviceLink) and Toyota have decided not to implement CarPlay and Android Auto in their cars, other manufacturers have yet to decide. PSA Peugeot Citroën, Honda, Subaru, and Mazda are reported to be considering adopting a similar approach based on the SmartDeviceLink platform. Yet some manufacturers welcome the fact that by adopting a third-party smartphone integration platform in their vehicles, they will avoid a major and expensive research and development headache.

However, it's highly unlikely drivers will accept anything less than a seamless transition between smartphone experience and dashboard experience, and eventually pressure will be put on manufacturers to relent. Our conversations with manufacturers suggest that they recognize this shift as being inevitable and rather than try to fight it they are seeking to embrace it.

Another strategy being debated by manufacturers is around the applications themselves. If manufacturers could launch their own applications, they would have the ability to create increased functionality beyond that of the third-party applications, thus providing a differentiator. How successful a strategy this will become remains to be seen, as ensuring the security of these applications would be essential.

The maturity of application security process between ISVs and manufacturers is another area of competition. Skilled people and proven processes and tools are needed to streamline the creation of secure software – all of which will require investment by manufacturers to compete with ISVs that have been investing in these for some time.

Driver Aid Security Questions

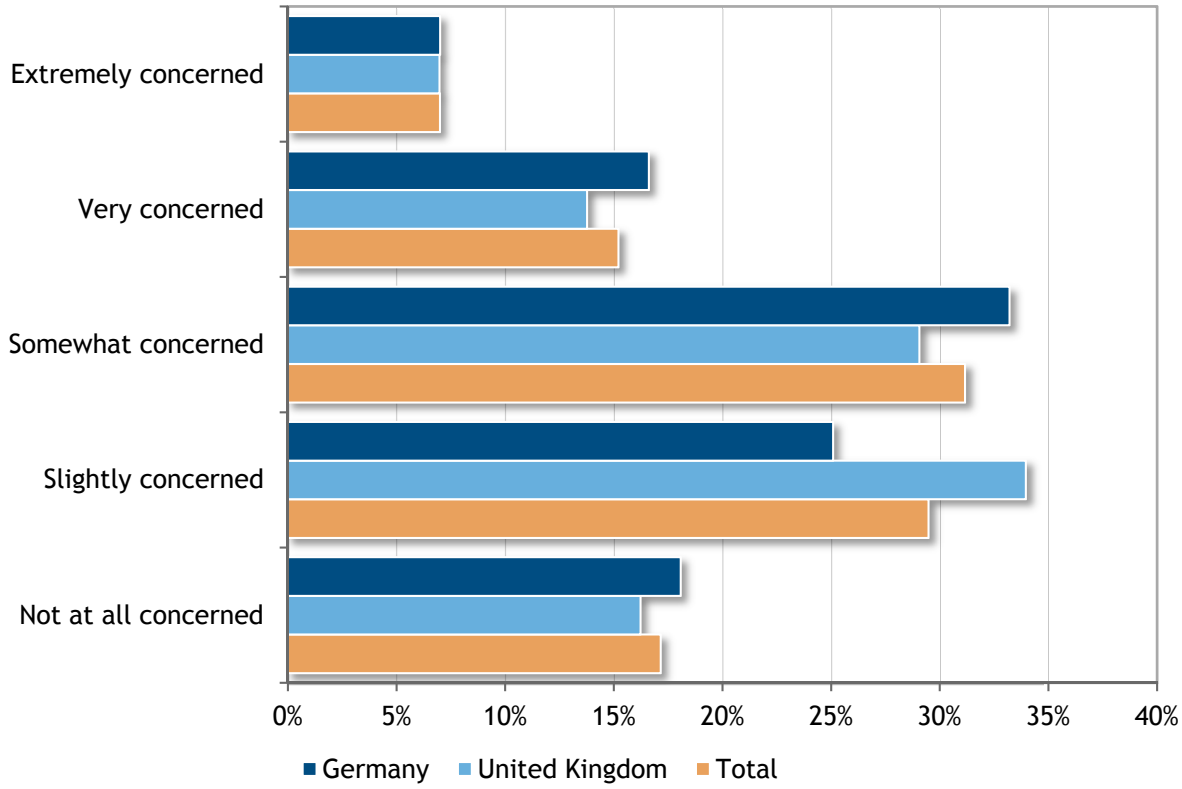
Unsurprisingly, manufacturers take the security of driver aids (e.g., adaptive cruise control, self/assisted parking, navigation-linked transmission) very seriously. Based on our conversations with manufactures, the preference is to keep software that provides driver/vehicle functionality separate from the infotainment systems that encourage downloadable applications. All of the various forms of integration platforms available today permit only an approved subset of smartphone applications to be accessed in the vehicle for an added layer of security. Further, these systems would not be allowed to connect wirelessly to the Internet and force software updates to occur via a physical connection at the dealership (or other trusted network). The primary concern here is that should vehicle performance be compromised in a cyberattack the consequences could be catastrophic. One needs only look at the incident with the Jeep Cherokee as an example, in which hackers accessed the Internet-ready radio in the infotainment system and broke rudimentary controls meant to prevent access to the performance harness.

In the research IDC undertook with drivers, the largest respondent group (around 30% in both countries) were “somewhat concerned” that such aids could be hacked and fail to operate as intended. If you then also include those who were “very concerned” and “extremely concerned” the total increases to over half (57%) in Germany and half (50%) in the UK.

FIGURE 1

Cyber Security Concerns

Q. How concerned are you that these systems could be hacked and fail to operate as intended?



Source: IDC, 2016

The vulnerability of such systems, especially those that take input from external data sources, is something that the vehicle manufacturers need to put the highest importance behind when it comes to security investment. As new technology becomes more common, making the connected car less driver-dependent (e.g., the BMW 7 Series smartphone app through which the driver can remotely park their car), manufacturers are going to need to start designing systems from day one with security as a key element, rather than a bolt-on afterthought.

Cyber Liability in Connected Cars

The cybersecurity challenge over connected cars is being further complicated as legislators hammer out laws to accommodate the usage of the new technology and transfer of liability. Questions include: Who should be held responsible if an application download to a car from a manufacturer approved site – or linked smartphone – has a vulnerability and puts the safety of the car or your personal data at risk? What constitutes “reasonable” efforts to address vulnerabilities in applications? What liability does the driver assume and how will car insurance change based on answers to these questions? Does the government have a duty to change road traffic laws?

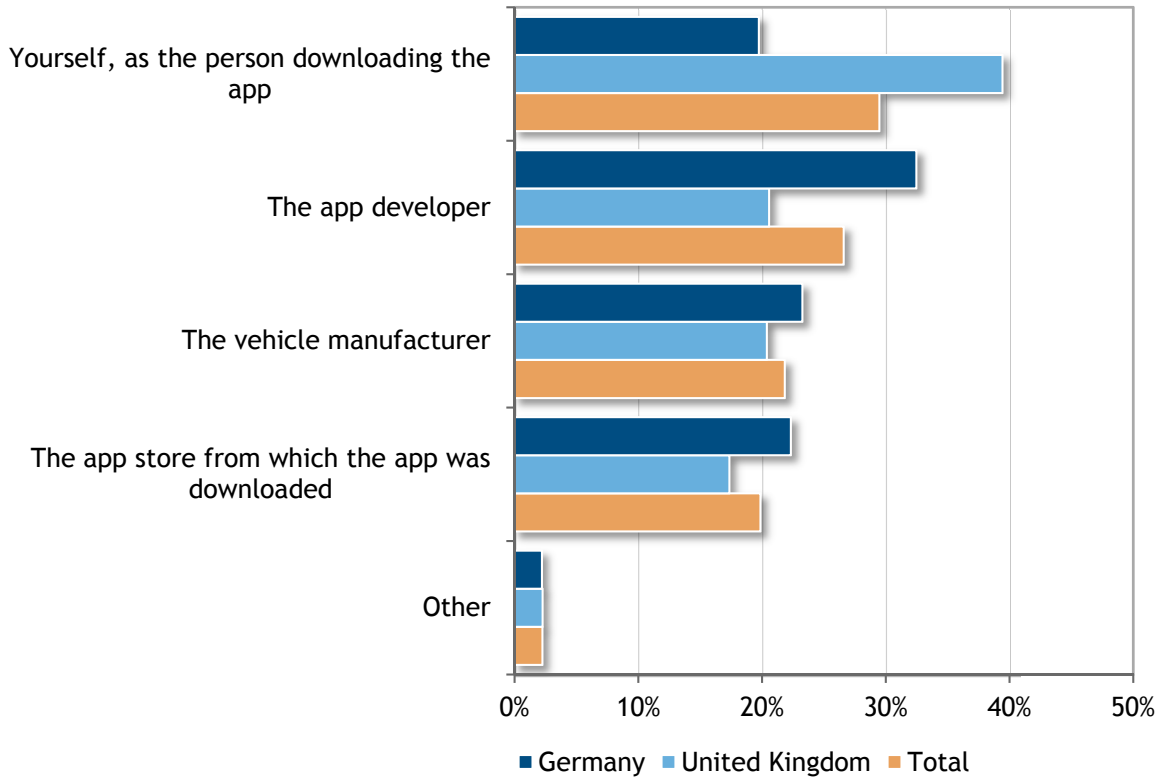
A common theme among all manufacturers we spoke with is around separating the infotainment system from the performance system, and this is mainly due to the ability of applications to be downloaded to the car or otherwise "leave the control of the manufacturer." This is similar to a smartphone provider that will take responsibility for the performance of a handset, but not the applications a user installs. Yet some manufacturers do not believe that this division can truly be guaranteed, so the question of who takes responsibility for the quality and security of the applications that drivers download must be raised.

Drivers have already made up their minds around the liability question, with significant differences in both surveyed countries. When considering who would be liable for a vulnerability in an application downloaded by the driver, nearly a third (32%) of drivers in Germany would hold the app developer responsible while for a quarter (23%) it's the vehicle manufacturer, and for 22% the app store where they downloaded it. While only a fifth (20%) think they themselves should be liable.

FIGURE 2

Cyber Liability

Q. Who should primarily be held responsible if an application you download to a car from a manufacturer-approved site — or linked smartphone — has a cyber-security vulnerability and puts the safety of the car or your personal data at risk?



Source: IDC, 2016

Drivers in the UK appear much more willing to put their hands up, with the majority of drivers (40%) holding themselves responsible, while a fifth of respondents point a finger at the app developers and manufacturers alike, and just 17% look to the app store. So while British drivers may be more

willing to hold themselves to account, almost two-thirds will still blame third parties, whether it is the application developer, and stores, or the manufacturer, all of which might actually become the very same company in the near future.

More generally, there is acceptance that issues surrounding liability need to be resolved sooner rather than later, but that there is a high degree of uncertainty. Manufacturers are pragmatic and accept that, from a consumer protection point of view, they retain a high degree of liability, if not with the originating fault or malfunction then at least with the responsibility for resolution and remediation.

One thing is clear: technology developments are taking place faster than the lawyers can bring in new legislation to accommodate the developments, and that is likely to be case for some time. This does not, however, absolve the manufacturers of responsibility to ensure their vehicles remain safe and reliable at all times. It is therefore imperative that manufacturers not only test their software to the extreme, but also ensure that software in the car is protected in such a way as to prevent external interference.

Personal Data and Privacy

There is also the important element of data privacy and whether the connected car will become yet another avenue for criminals to gain large volumes of consumer data. Attitudes towards this issue among the drivers we spoke to seem to be very much in line with their thoughts regarding similar issues when using a smartphone. The manufacturers we spoke to are conscious of this, although feel that it's not a problem they need to worry about.

Even if this might be the case now, developments are pointing into another direction as most of the services enhancing driver experience will need to rely on personal data. Navigation systems allowing to find, reserve, and pay for parking are just one example; being able to connect navigation and a business calendar is another. Data on drivers' movements, such as time of travel, destination and speed, may be captured by the vehicle and relayed to a central computer store, and the protection of this information becomes vital (and falls under new wide-ranging EU General Data Protection Regulation [GDPR]). Importantly, GDPR has a very broad definition of personal data (much broader than that in the US, for example) which would include aggregated data that collectively identified an individual and/or their movements.

Our interviews with the manufacturers show they are certainly aware of data protection and privacy issues as they relate to gathering personal data from vehicles. What is interesting is their comments with regard to the collection of data.

It seems very likely that data relating to vehicle journeys would be gathered in order to provide traffic, road condition, weather, and other location-specific information. The question is how long this data be will collected, for what purpose, and whether it is sent to a central location as input to analytics. The latter is specifically important after the European Court of Justice has recently invalidated the Safe Harbor agreement and focuses attention on the legality of international data transfers. Many ISVs have underpinned their entire business models on collecting just user data – think Google, Apple, and Amazon – so it's a fair bet this will extend to any applications used by drivers. However, there is recognition among manufacturers that a balance needs to be struck between data protection and the sharing of data – for example, to alert other drivers to traffic jams – and this is not really any different to the challenges faced by the smartphone community and location-based data from users.

The results are a recognition that privacy sensitivity will vary from country to country, as we see in our driver research. However, EU legislation is being enhanced to require a similar (and higher) level of privacy in all EU countries. The GDPR brings a consistency to EU data privacy law across

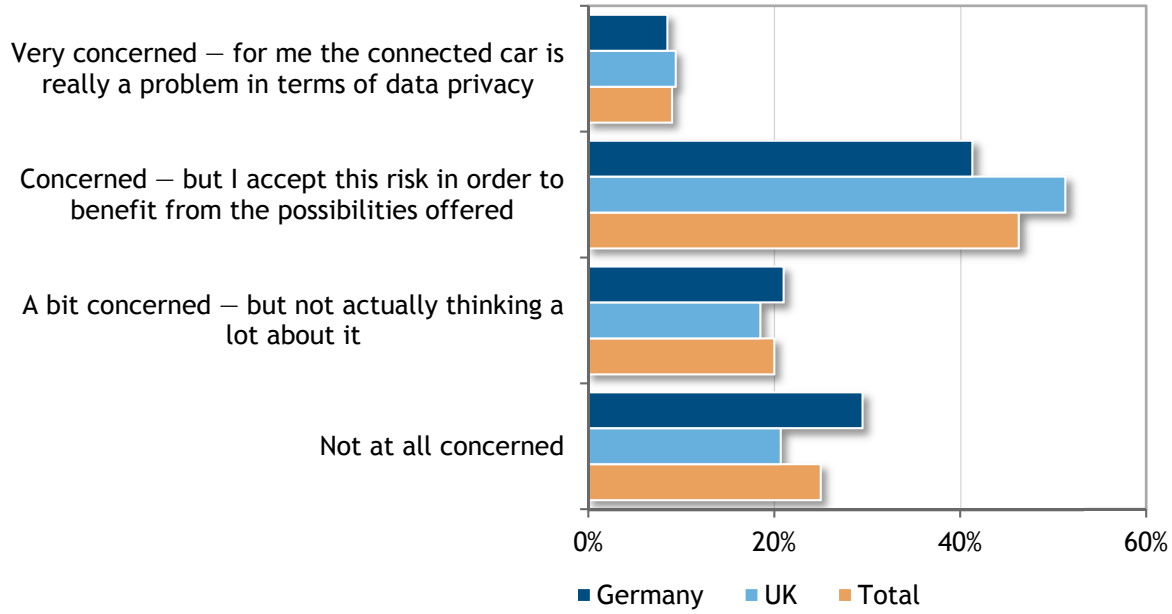
all 28 member states, and also applies equally to both data controllers and third-party data processors. This has repercussions for manufacturers and ISVs as data gatherers/aggregators and any third-party service provider that uses this data to provide services to drivers and other customer types (such as insurers). The balance, at least in Europe, is tipping toward more, rather than less, privacy.

Our interviews with drivers show that a large proportion are "somewhat concerned" about their personal information being shared, though they admit that this is not something they have spent a lot of time thinking about. The majority of German drivers (41%) and British drivers (51%) are "concerned" or "very concerned" about this issue. Roughly the same proportion of British and German drivers (18% and 21%, respectively) are "concerned" regarding personal data, but accept a degree of risk in order to benefit from the possibilities of the connected car. The balance (30% in Germany, 21% in the UK) are "very concerned" and regard the connected car as a major problem in terms of data privacy. This is an interesting result: data privacy is often characterized as a uniquely German issue, but our research shows that one-fifth of British drivers are also "very concerned" about data privacy protection in the connected car.

FIGURE 3

The Connected Car and Privacy

Q. How concerned are you that personal data collected by a connected car could be used in ways you did not intend it to?



Source: IDC, 2016

What Apps do Drivers Want to Have in Their Vehicles?

From our discussions, most manufacturers think that when it comes to downloadable applications their primary domain is in navigation aids, and most are unlikely to offer social media and entertainment applications. With most manufacturers there is a strong division of perceived role in downloadable functionality, between core automotive capability and infotainment.

The manufacturers' position seems to be in line with their customers' as the research shows application preference is related primarily to enhancing the driver experience, rather than entertainment. The majority of drivers polled in our survey would most likely download apps for navigation (74% in Germany, 69% in the UK), and travel information (55% in Germany, 52% in the UK). Drivers also seem keen on downloading performance-enhancing apps: to help avoid dangerous weather conditions (40% in Germany, 44% in the UK) and find parking (56%; 47%) as well as to enhance speed (27%; 30%) and fuel economy (48% in both countries).

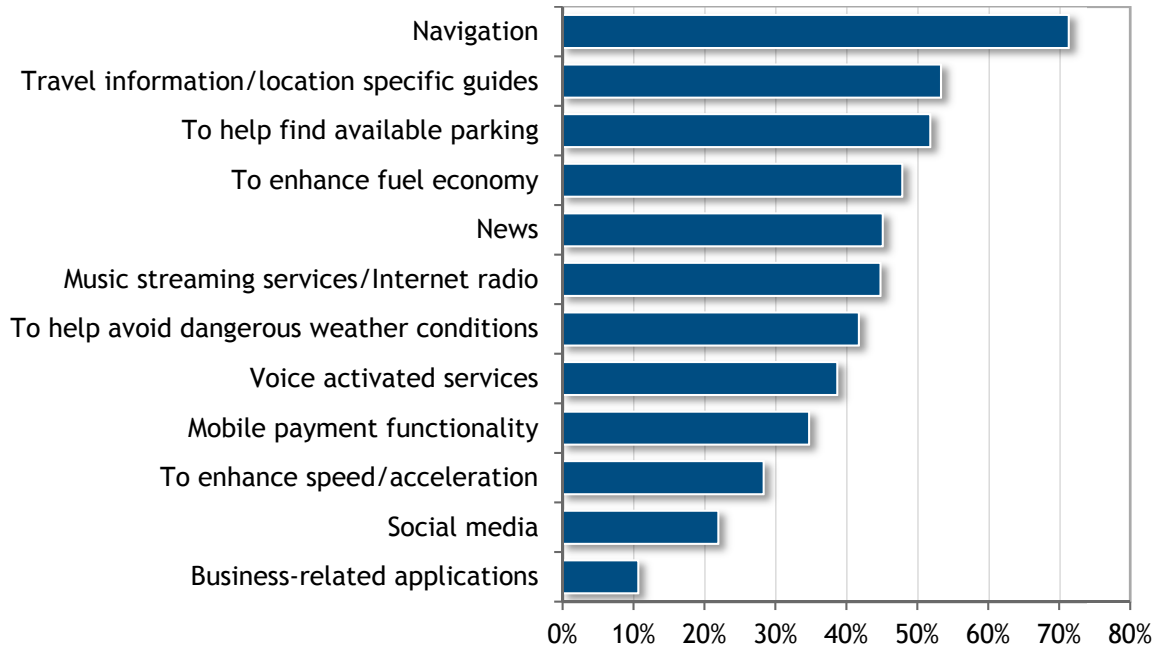
By far the most popular application is navigation, already one of the most frequently used features in today's vehicles. Presumably, drivers anticipate even better navigation, and an enhanced mechanism for downloading additional navigation utilities, such as updated maps, routes and points of interest. Second in application preference is travel information, such as location-specific guidance, traffic and congestion updates, and other driver-based data. This seems sensible, and together with navigation would enhance the overall information provision for drivers (see Figure 4). These application preferences are followed by the ability to find available parking, and to enhance fuel economy.

Other applications that seem popular with drivers are news services and music streaming radio services. Payment capability, social media, and business-related applications seem to be much less in demand.

FIGURE 4

Driver App Preference

Which applications would you download to replace or augment the functionality of your car?



Source: IDC, 2016

Summary and Conclusions

Today is one of the most exciting times for the automotive industry, yet its leading manufacturers face arguably one of their most significant challenges since its inception. With the development of the connected car showing no signs of slowing, and in an era in which delivering a first-class user experience is front of mind for all organizations across all sectors, car manufacturers face unprecedented competition for market share from software companies.

Not only are technology companies developing in-car software platforms and applications, the likes of Google and Apple are already taking strides in the development of their self-driving automotive prototypes, taking the first steps directly into the car manufacturer market.

Manufacturers cannot afford to be complacent when it comes to software and application security. Based on our research, they appear to be ahead of the concerns drivers have, which is a good sign. However, the manufacturers acknowledge a difference between concern and understanding of the issues, and a readiness of the technology to deliver on these. From our interviews, we predict a suggested timeframe of one to three years before connected car systems are implemented with full consideration to cybersecurity concerns. The question for manufacturers is whether this is realistically feasible given the challenges ahead and the rate at which applications are being developed today.

Clearly the concerns over cybersecurity arise when considering driver aids, as the consequences of successful cyberattacks are likely to be severe. Manufacturers are considering two approaches to securing this kind of technology. The first is to completely separate infotainment systems, which are assumed to be supplied predominantly by third-party application developers, from driver functionality. The second approach is for the manufacturer to assume responsibility – if not liability – for the complete car "package." There are pros and cons of each approach, but our research suggests that drivers are unequivocal about where they place responsibility: firmly in the hands of manufacturers. It therefore seems that manufacturers need to grasp this nettle firmly, and have a collective as well as individual approach and response to security concerns.

With regard to data protection and privacy issues, drivers appear increasingly sensitive to this subject. Although German drivers are more concerned than their British counterparts, the overall levels of awareness and concern are significant. Manufacturers, too, are fully aware of their obligations in addressing the privacy concerns of drivers. Yet we detected a relatively relaxed attitude here, which IDC finds surprising. Some manufacturers don't expect to collect or store any private data from customers, thus avoiding the issue altogether. This we see as unlikely given the amount of data that could be collected and the variety of purposes for which this data could usefully be used. We also saw recognition of a balance between strong privacy and the utility of shared data.

In short, we think that manufacturers' views on privacy are not yet fully formed, and although they are aware of drivers' concerns and their own responsibilities, the structures and processes to manage private data are not yet in place. Manufacturers need to address this issue with some urgency: they must anticipate collecting data and understand fully the legal and moral obligations to drivers.

The positive implication from our research is that the market for downloadable apps is large, spanning the entire market of drivers of all ages and genders. Manufacturers are, we think, correct in focusing on apps that enhance car functionality, such as the many driving aid apps currently being developed. They should continue to leave the infotainment segment to the strong players in that sector: predominantly Google and Apple. But they cannot abdicate security to these third parties.

Our conversations with drivers and manufacturers have cast interesting insight into the ways in which new software-based technologies will be offered by suppliers and adopted by consumers. The prevailing view among drivers was very much in support of apps that enhance the driver experience, such as assistance in finding parking spaces (or even in parking the car autonomously), as well as navigation and fuel economy. Similarly, the manufacturers see their role primarily in enhancing the driver experience through extended functionality. They see a distinct difference between car function and infotainment, and seem willing to cede development and supply of the latter category of app to the likes of Google and Apple.

Methodology

For this study, IDC conducted in-depth interviews with leading vehicle manufacturers and automotive industry representatives, including ADAC (leading German automotive industry association), Bosch, Delphi, Fiat-Chrysler, Scania, and Seat.

Further research was conducted into the perceptions of vehicle drivers based equally in the UK and Germany. We conducted 1072 interviews across a broad range of demographics (age, gender, location). The research and interviews were conducted in November and December 2015.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com