BearingPoint® Institute

TRENDS

#connectedcar

# Connected cars and privacy: shifting gear for GDPR?

## OEMs need to engineer their vehicles and connected car ecosystems for compliance and customer experience

## IN 30 SECONDS

- In the era of the connected car, OEMs need to transform their approach to customer data, address privacy concerns and comply with regulation especially regarding the new GDPR
- These challenges are compounded by rapidly evolving privacy regulations, and the difficulty of changing mindsets within well-established businesses
- We provide six recommendations for vehicle manufacturers to rethink their fundamental approach to privacy and establish it as a core tenet of their businesses

### The GDPR – Time to act

The General Data Protection Regulation (GDPR) applies to data controllers and data processors established inside and outside the EU, whose processing activities relate to the offer of goods or services to individuals in the EU...

**...but businesses are seriously underprepared**

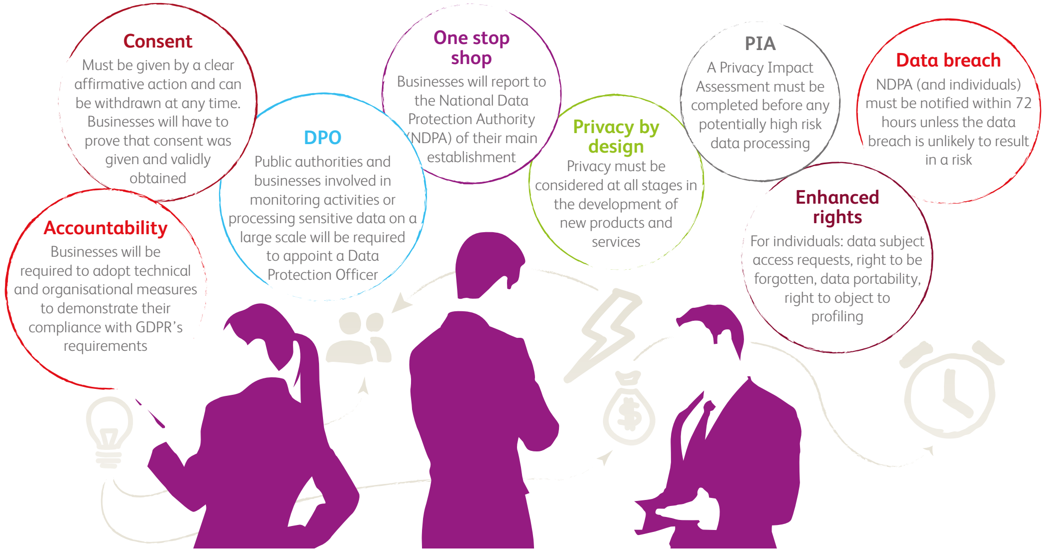
**96%**
Do not fully understand GDPR

**9 in 10**
Have concerns in their ability to become compliant

**€20million**
Fines of up to 4% of annual global turnover or €20 million

**25 May 2018**
Date which GDPR is directly applicable

**Key changes you should be aware of:**



**Consent**
Must be given by a clear affirmative action and can be withdrawn at any time. Businesses will have to prove that consent was given and validly obtained

**Accountability**
Businesses will be required to adopt technical and organisational measures to demonstrate their compliance with GDPR's requirements

**DPO**
Public authorities and businesses involved in monitoring activities or processing sensitive data on a large scale will be required to appoint a Data Protection Officer

**One stop shop**
Businesses will report to the National Data Protection Authority (NDPA) of their main establishment

**Privacy by design**
Privacy must be considered at all stages in the development of new products and services

**PIA**
A Privacy Impact Assessment must be completed before any potentially high risk data processing

**Data breach**
NDPA (and individuals) must be notified within 72 hours unless the data breach is unlikely to result in a risk

**Enhanced rights**
For individuals: data subject access requests, right to be forgotten, data portability, right to object to profiling

# #connectedcar

While many original equipment manufacturers (OEMs) have got up to speed quickly with the data protection requirements which come with connected vehicles, a new piece of European legislation with global implications will mean they must shift gear to ensure they are compliant. Data plays an increasingly important role for OEMs, so ensuring that they comply with the General Data Protection Regulation (GDPR), through a strong privacy strategy is essential. Without this, their ability to harness the value of the data their vehicles produce will be deeply compromised.[2]

Developing a compliant approach to data privacy while at the same time delivering a compelling customer experience is mission critical for connected-car manufacturers. Valuable lessons may be learned from sectors that have already sweated over the best ways to protect customer privacy and instil customer trust. Yet vehicle manufacturers also face a unique set of hurdles, given the level of disruption brought about by connected cars. We believe the Holy Grail for OEMs is a strategy that addresses privacy holistically and transparently, which goes beyond merely complying with legislation such as the GDPR. Reaching this stage will not be a simple process, but it is essential as if an organisation fails to comply with the GDPR it can be fined 4% of its annual global turnover.

## Identifying the privacy challenges

In November 2015, Allgemeiner Deutscher Automobil-Club (ADAC), the German motorist organisation, discovered that large amounts of data were being captured by the on-board diagnostics (OBD) system of a BMW320d, including driving destinations and phone contacts, without the permission of the user.[1] Other models will doubtlessly have the same issues – previously, this data could only be accessed by directly connecting to the OBD, but now the data is starting to be transmitted wirelessly – and the amount of data being captured is growing by the day. Explicit customer permissions is a core principle in GDPR. OEMs must ensure that connected car data is not captured, processed and shared without a customer proactively opting in. This is just one of the privacy challenges that confront connected-car teams.

## Evolving relationships

As connected cars move to the mainstream, OEMs will have to deal directly and around-the-clock with consumers – a sharp contrast from previous, sporadic interactions through dealerships. An important part of this new relationship will be based around data, which will flow automatically from car to manufacturer.[2] This means that OEMs need to learn how to handle large volumes of data – more than 25GB per hour per car, according to some estimates[3] – as well as deal with consumer concerns over how that data is being used, stored and shared.

*OEMs need to learn how to handle huge volumes of data – more than 25GB per hour per car, according to some estimates*

Doing this well will mean significant organisational changes for OEMs. Software is already becoming a key differentiator[4] for customers when making decisions about which new car to buy.[5] As OEMs add more software to their cars, there will be new services to manage and more data to analyse, store and secure – a serious shift from the old hardware-focused days. The organisational structure of car manufacturers will increasingly change to reflect these changes. Building privacy and data governance into these new structures should be a high priority.

# #connectedcar

Whilst the first challenge was building the right infrastructure, teams and individual capabilities to handle data comprehensively and thoughtfully, OEMs are now faced with a new challenge having to adapt their systems to the requirements of the GDPR. A clear appreciation for data protection, and in particular the details of the GDPR, will be required, as many in the industry are not yet familiar with existing regulations and internal policies. This can lead to miscommunications with the public, which does nothing to put privacy fears to rest.[6]

## A changing ecosystem

Vehicle manufacturers are scrambling to find their place in a highly dynamic ecosystem of connected-car services – having to determine which services to provide to customers, and with whom they should partner to achieve this. A central question concerns which connected services should be developed in-house and which should be fielded out to partners and third parties. External companies, for example, may be less rigorous than the OEMs in attending scrupulously to secure data management as they are not the data controllers. In the event of a problem it is the OEM that will bear the brunt of the reputational damage, not the service provider. Beyond reputational risks, it is the OEM again, not the service provider, that must answer to the National Data Protection Authority and become liable for the fines in cases of infringement. This has major implications for the privacy strategy of manufacturers.

Importantly, access to customer data won't just be confined to external digital service providers. As the connected-car ecosystem matures, cars will increasingly communicate with pedestrians, public infrastructure (such as the Safespot project currently being trialled in Europe, which creates dynamic networks between vehicles and infrastructure to improve safety[7]), and other cars – including some from different manufacturers. Ultimately, this will lead to a vast number of interconnections where the privacy of the consumer must be considered and protected – yet another reason to develop a holistic privacy framework.

## Creative tensions

One of the biggest challenges around privacy is that it brings a new set of interests into the development process. Engineers, naturally, want to design innovative products that use customer data in novel and exciting ways, and may be less aware for data privacy compliance. This can create conflict with legal teams, who strive to minimise risk in such projects and the OEM's potential liability. Similarly, marketing teams have their own set of priorities: how to harness data to grow their insights about customers and vehicles, and how to sell these innovations.

> *In the event of a problem, it is the OEM that will bear the brunt of the reputational damage – not the service provider*

At present, legal teams tend to be disconnected from the development phase of projects, often brought in late in the process once the product or service has already been developed. This can lead to situations where a project is eventually deemed unviable from a legal perspective after engineers have worked on it for months, serving to undermine the relationship between the two departments as a result. A holistic privacy framework would stop these issues before they even start.

#connectedcar

# RECOMMENDATIONS

In October 2015, Volvo announced it would accept full liability for its cars when they are driving in autonomous mode.[8] This move represents a landmark for connected cars, effectively removing one area of concern for consumers as they make purchasing decisions on new cars. Now, OEMs need to make the same leap forward for privacy.

In order to deal with privacy issues in a holistic way which complies with the GDPR, OEMs must address a number of challenges and change their structures to accommodate privacy across the whole business. But where to start?

## 1. Becoming GDPR compliant

To be ready for the GDPR coming into effect in May 2018 OEMs must start planning and acting now. To begin with, they should review the legislation to understand its implications. As OEMs are still navigating how to best use connected car data for customer and business value, complying with the GDPR adds additional complexity. Establishing the amount of effort required at the beginning to cover the full scope of personal data used across the business is vital to ensuring a successful compliance project.

Carrying out an audit of the personal data an organisation holds and processes is a critical first step to understanding what data is held, where it originated and who it is shared with. Connected Car initiatives have driven OEMs to ask customers to sign a Connected Car Privacy Policy as part of their account set up. These must be reviewed to ensure they are in line with GDPR requirements with particular attention paid to the rights which individuals have. Do policies afford individuals the ability to request the data that is held about them? Can individuals correct their data? Are individuals able to delete their data?

Deletion of data is a particularly thorny issue. For OEMs to provide Connected Car services they are often required to transfer and store data across multiple different platforms and to share data with suppliers. The surfeit of data processors means that OEMs must implement particularly robust processes to allow them to comply with customers' requests that their data be deleted. Moreover, such requests have to be balanced against requirements to retain data to protect OEMs against litigation.

Another important consideration is whether the current processes ask customers for their consent to be contacted directly based on vehicle diagnostic information and consent for this data to be shared with the dealer network and to receive proactive communications? These are only some of the rights which individuals have because of the GDPR. However, drafting a compliant Privacy Policy is only half the battle – the critical question for organisations is if they have the processes in place to allow individuals to exercise their rights? Deletion of data is a particularly thorny issue. For OEMs to provide Connected Car services they are often required to transfer and store data across multiple different platforms and to share data with suppliers. The surfeit of data processors means that OEMs must implement particularly robust processes to allow them to comply with customers' requests that their data be deleted. Moreover, such requests have to be balanced against requirements to retain data to protect OEMs against litigation.

Implementing the required processes is essential for organisations to understand their data flows – they can do so through mapping where their data is sent. This will allow them to identify any weaknesses in their data security and IT infrastructure. Once all of this is understood they should draft and prioritise a set of initiatives which will enable them to become GDPR ready.

BMW recently launched CarData, positioning itself at the forefront of GDPR compliance. This new service provides a high level of transparency, security and puts their customers in control of their telematics data. Customers are provided with a summary of the data sent by their vehicle to BMW ConnectedDrive system, and a view of the latest version of their data. They can also request that their data be archived and have the option to share their data with third parties.

•••

## 2. An executive-level commitment to privacy

Privacy must become an integral part of every OEM's company vision, and a core component of the company culture. Despite some recent initiatives, this is yet to be the norm industry-wide. The first step in this direction is reaching consensus at board level that privacy must be managed comprehensively, at every stage of connected-car development and beyond. Once this is attained, OEMs will be in a position to begin securing data at every stage of the value loop, within every node of the organisation.

The next step is appointing a data protection officer to the C-suite, who will be responsible for developing a company-wide privacy programme to deliver GDPR compliance to historical data and all future data initiatives. Companies can then implement a privacy committee or centre of excellence, install privacy champions in every department, build training plans for privacy awareness, and run regular privacy audits across the business.

## 3. A holistic approach to Privacy by Design

First conceived in 1995, Privacy by Design (PbD) has shot to prominence in recent years thanks to the advent of big-data technologies, and their implications for consumer privacy. At the heart of PbD is the idea that privacy should be taken into account throughout the whole engineering process, rather than tacked on at the end. PbD is now widely accepted by regulators around the world as a fundamental aspect of privacy protection and is key concept in the GDPR.

PbD brings many benefits to organisations that adopt it into their engineering processes. First, it engenders increased awareness of privacy issues within businesses. Second, it assists companies in identifying potential privacy issues at an early stage of development. This will help minimise projects being scrapped belatedly as non-viable from a privacy perspective.

To implement PbD, clear communication channels need to be established – whereby information on current regulations informs the planning of design projects, and an appropriate and structured review process is in place that involves the relevant stakeholders, including product development teams, connected-car teams and legal departments. This approach must also be pragmatic: managing customer expectations over privacy must be weighed against the seamless experience that connected-car technologies will provide them with.

Many technology leaders already incorporate PbD into their existing development processes. Facebook's Chief Privacy Officer claims that the company incorporates PbD principles into every product, feature and update it now builds.[9] Apple encrypts all outgoing messages from its iPhones without storing the unique encryption key, meaning the company couldn't hand the keys over to the authorities even if it wanted to.[10] OEMs must hold themselves to the same standards as these privacy leaders.

*In October 2015, Volvo announced it would accept full liability for its cars when they are in autonomous mode. OEMs need to make the same leap forward for privacy*

## 4. Rethink and retool legal

Privacy issues demand legal solutions. As well as the traditional duties of negotiating contracts with suppliers and defending their employer from lawsuits, OEM legal teams must become advocates for customer privacy in the new environment of PbD – a drastic change in both culture and scope. Much rides on whether legal teams can resist acting as blockers to bright ideas, and instead act as facilitators of innovation just as they continue to foster privacy awareness.

Nowadays, when a vehicle manufacturer is deciding which new connected services to offer, it is the job of legal to advise on what can be done from a data protection point of view, in addition to what the customer privacy expectations are in that domain. For this to be more effective, legal teams need to become better integrated into the strategy, design, development and engineering phases of connected-car teams. They will also need to learn, speak and teach a new language: privacy. All of this requires that legal professionals possess skill-sets in these areas - presenting a new hiring and training challenge for OEMs.

To that end, vehicle manufacturers should create connected-car data privacy roles that get involved at every stage of the product development and launch process. To supervise this team, there should be a connected-car data protection officer who would report to the company's new C-level data protection officer. Qualified lawyers with expertise in contracts, data protection and an understanding of the GDPR then need to be brought on board. This team should sit in the connected-car business unit and have a deep understanding of the services being developed. In this way, it should be able to offer targeted legal advice and, most critically, direct and realign development based on regulatory compliance.

## 5. Keep an eye on changing privacy regulations

The GDPR is just one example of how privacy legislation is evolving data legislation also changed in Russia in 2016.. Even small changes in policy can have immediate and disruptive effects for OEMs.

To ensure compliance with the GDPR and any legislation which may follow, and therefore mitigate the risk of legal challenges, vehicle manufacturers must extend the remit of existing compliance teams towards data protection and the digital environment. The first role of these new teams should be to monitor regulatory changes worldwide that impact customer data protection, and communicate these changes to the relevant stakeholders before they come into force. The team should then provide instantaneous impact assessment on data regulation compliance for every change, across every country and product. This should help unearth the changes that need to be made, and lead change across the business.

The second role of these teams should be to influence and lobby regulatory bodies to push data privacy in a direction that will benefit the current business strategy of the OEM. These new roles will require different skillsets from the teams managed by the OEM's Chief Compliance Officer, which will require the recruitment of lawyers expert in data protection, as well as lobbyists and compliance analysts.

OEMs would do well to look at Microsoft as an example of a global company implementing these privacy measures effectively. The company has a 'global privacy community' composed of privacy champions, leads and managers, who give advice across the whole business on privacy-related issues. Each business group is responsible for ensuring that it is compliant with corporate privacy requirements, with mechanisms in place to ensure this happens, including training, privacy identification tools, and an escalation response framework.[11]

•••

## 6. Make privacy a core tenet of the brand

At the heart of all these privacy issues is the need to design connected-car services in a way that allows customers to exert meaningful control over their personal data, whilst maintaining their enjoyment of the services provided.

This means developing a forthcoming, informative privacy policy and set of terms and conditions for consumers. This is an area where OEMs can learn from best practices: Uber and Facebook, for example, group their privacy settings in easy-to-read modules, and use a multi-layered approach. As standard practice in these companies, each privacy setting can be summed up in one sentence but, if customers click through, they have access to extended information. New policy changes are explained clearly to customers in one email, with an opt-in box to click.

A key function of privacy settings already available from leaders and required by GDPR is the ability to easily opt out of the connected-car services, erasing all customer data and details collected, as well as the ability to download all the data that a company has collected from them.[12] OEMs must now adopt this as standard.

But in order to reach the next level of customer engagement when it comes to privacy, OEMs could also consider public awareness campaigns: from infographics to privacy FAQs and videos – anything that enhances the OEM's profile as a privacy leader will go a long way to boosting the culture of privacy in the organisation.

However, learning from other sectors will only take vehicle manufacturers so far. A mobile phone, for example, typically only has one user over the course of its lifetime, but a car could have multiple users and multiple owners. How can OEMs ensure that every time a person gets in the driving seat, they have accepted the privacy policy for each service? Should the customer assume their data will always remain private unless specifically told otherwise? These are questions to which OEMs must find answers.

#connectedcar

# Conclusion

The risks for OEMs of getting privacy strategy and compliance wrong are high, as the consequences are spread across a number of areas: substantial fines (up to 4% of annual global turnover or €20 million), compliance risk, reputational risk, and the threat of alienating customers with high expectations when it comes to privacy protection. But this is also an opportunity for OEMs to rise above their competitors. By being the manufacturer that really 'gets' privacy, they stand to make huge leaps in terms of both customer loyalty and brand image. But in order to do this, privacy must be instilled into every step of the connected-car development and design process – anything other than a holistic approach will ensure that OEMs are always on the back foot, putting themselves in the way of risk, and missing out on huge opportunities to gain a lead on their rivals.

Although OEMs can undertake a number of measures to address the privacy concerns of customers, the fact is that the concept of privacy has shifted and will continue to develop, as technology opens both individuals and companies up to the transparency of the connected world. The GDPR establishes some basic principles and good practices for businesses to protect their customers. OEMs must embed these principles and processes as the starting place, but they should also continue to challenge their own collection and use of customer data. They must focus first on building a compelling and transparent customer experience and build trust with customers so that the acceptance and use of connected car services continues to grow and pave the way for the autonomous future.

*How can OEMs ensure that every time a person gets in the driving seat, they have accepted the privacy policy for each service? Should the customer assume their data will always remain private unless specifically told otherwise? These are questions to which OEMs must find answers*

## KEY TAKEAWAYS

- Connected cars will change the relationship between the vehicle manufacturers and their customers – for the first time, they will communicate around the clock, and directly
- They will also change the nature of the OEM ecosystem – new players will emerge who want access to customer data in return for advanced products and services
- Keeping customer data safe will mean bringing the legal team into a bold new position within the OEM – and this will bring its own challenges of culture and integration
- The key to protecting customer data will be a holistic data privacy strategy – OEMs must integrate privacy into their culture and processes
- Legal teams will need to be completely re-shaped and integrated within connected-car teams
- In the boardroom, with appointments and policies that acknowledge the importance of protecting the privacy of their customers
- Legal teams will need to be completely re-shaped, and integrated within connected-car teams
- OEMs will need to keep a watchful eye on ever-evolving privacy regulations around the world to ensure their products match international compliance expectations
- Vehicle manufacturers can use privacy by design principles to create a holistic and pragmatic approach to privacy
- Overall, though, privacy must become a core part of the OEM's brand
- This must translate into a smooth, easy-to-understand experience for the customer

## About the authors

**Matthew Roe**
Senior consultant, BearingPoint, London

Matthew Roe is a senior consultant at BearingPoint in London. He has led a number of privacy reviews to help organisations enter markets across Europe, Asia and South America. He has also managed several initiatives to improve data privacy processes and to ensure customer interests are kept front of mind.

matthew.roe@bearingpointinstitute.com

**Capucine Nivet**
Senior consultant, BearingPoint, London

Capucine is a senior consultant at BearingPoint in London, specialising in managing data protection and privacy processes and risks, particularly in the automotive industry. She has led a number of data protection projects, ranging from implementing multi-jurisdictional privacy policies for the worldwide rollout of new connected car services, to designing and delivering privacy awareness training and advising on customer complaint-handling.

capucine.nivet@bearingpointinstitute.com

**Sarah-Jayne Williams**
Partner, BearingPoint, London

Sarah-Jayne is a Partner at BearingPoint and leader of the Digital Customer Management practice. Specialising in automotive, she works closely with OEMs and automotive leasing providers alike to design and deliver digital strategies and connected car services. Sarah-Jayne has published work on digital customer behaviours and world-class digital organisations; she co-authored the book Addressing customer paradoxes in the digital world, published by Pearson. She is also a former winner of the Management Consulting Association's award for Marketing Consultant of the Year and a joint team winner (with Jaguar Land Rover) for the 2015 Management Consultancies Association Digital and Technology Project of the Year for Connected Car.

sarah-jayne.williams@bearingpointinstitute.com

#connectedcar

## Project team

Christophe Grosbost from BearingPoint.

## Acknowledgements

Matthias Loebich, Angelique Tourneux and James Dickson from BearingPoint; Tanja Schwarz and Sharon Springell from the BearingPoint Institute; Karim Meggaro from Longitude; Joe Barkai; Christopher Norris from CopyGhosting Editorial Services; Michael Agar from Michael Agar Design.

## Notes and Bibliography

1. ‘Connected cars don’t care about privacy, according to study’, Connected Car Tech, Bristol, UK, web, Ryan Daws, 27/11/15 http://bit.ly/CCT_CCprivacy
2. ‘How can vehicle manufacturers fit into the new connected car ecosystem?’, BearingPoint Institute, web, http://bit.ly/2rwQqL3
3. *The internet on wheels and Hitachi, Ltd*, Hitachi Data Systems, Santa Clara, CA, USA, web: PDF white paper, Hitachi Data Systems, 12/15 http://bit.ly/HDS_IonW
4. OEMs and connected-cars: time to seize the connected future, BearingPoint Institute, web, http://inst.be/008CCX
5. *Connected car in Europe: strategies and technologies for connected driving*, Pierre Audoin Consultants, Paris, France, web: PDF, Sarah-Jayne Williams and Matthias Loebich, slide 6, 2015 http://bit.ly/BPccinE
6. ‘Ford exec: “We know everyone who breaks the law” thanks to the GPS in your car’, Business Insider, London, UK, web, Jim Edwards, 08/01/14 http://bit.ly/BI_Ford
7. ‘Home page: SAFESPOT tab’, SAFESPOT, Torino, Italy, web, Roberto Brignolo, 2009 http://www.safespot-eu.org
8. ‘Volvo CEO: We will accept all liability when our cars are in autonomous mode’, Fortune, New York, NY, USA, web, Kirsten Korosec, 07/10/15 http://bit.ly/Fortune_Volvo
9. ”Facebook is a privacy enhancing technology” says Facebook’, Computing, London, UK, web (subscription only), John Leonard, 06/10/15 http://bit.ly/Comp_FBprivacy
10. ‘Privacy by Design: an idea whose time has come’, Computing, London, UK, web (subscription only), John Leonard, 02/10/15 http://bit.ly/Comp_PbD
11. ‘Trustworthy computing: our commitment’, Microsoft, Redmond, WA, USA, web: privacy commitment, 2016 http://bit.ly/MSoft_privcomm
12. ‘Trustworthy computing: practices’, Microsoft, Redmond, WA, USA, web: privacy practices, 2016 http://bit.ly/MSoft_privprac

#connectedcar

## About the BearingPoint Institute

At the BearingPoint Institute, our ambition goes beyond traditional 'thought leadership'. We aim to contribute original ideas to the science of business management whilst equipping decision makers with practical advice gained in the field and through our research projects.

www.bearingpointinstitute.com

## About BearingPoint

BearingPoint consultants understand that the world of business changes constantly and that the resulting complexities demand intelligent and adaptive solutions. Our clients, whether in commercial or financial industries or in government, experience real results when they work with us. We combine industry, operational and technology skills with relevant proprietary and other assets in order to tailor solutions for each client's individual challenges. This adaptive approach is at the heart of our culture and has led to long-standing relationships with many of the world's leading companies and organizations. Our global consulting network of 9700 people serves clients in more than 70 countries and engages with them for measurable results and long-lasting success.

www.bearingpoint.com

## CONNECT

Follow us on Twitter at @institute_be

Join us on LinkedIn at www.inst.be/linkedin

www.bearingpointinstitute.com

**Send us your comments, thoughts and feedback:**

editor@bearingpointinstitute.com

www.inst.be/feedback

## DOWNLOAD

Read the BearingPoint Institute on your tablet with the mobile app:

iOS version from the iTunes AppStore

Android app on Google Play

Amazon Kindle (Fire only) store

(to guarantee a good reading experience, these apps are for tablets only)