THE VALUE OF OUR DIGITAL IDENTITY

LIBERTY GLOBAL
Policy Series

BCG
The Boston Consulting Group

TABLE OF CONTENTS

KM

key messages

KEY MESSAGES

- In an increasingly digital society, personal data has become a new form of currency. The biggest challenge for political and business leaders is to establish the trust that enables that currency to keep flowing.

- "Digital identity" is the sum of all digitally available information about an individual. It is becoming increasingly complete and traceable, driven by the exponential growth of available data and the big data capabilities to process it.

- How digital identity develops is an important concern for consumers and companies alike. Individuals are worried about losing both their privacy and control over their personal data. Companies, on the other hand, fear that missteps – be it through their own, or third-party applications – could compromise their position as trusted provider.

- Global trends including the social media boom (a quarter of the world's population will be members of online social networks by 2015) and the burgeoning "Internet of things" (some 75 million machine-to-machine connections will be added in Europe by 2015) result not only in increased information volume, but also completely new types of data.

- From a macroeconomic perspective, it becomes clear that digital data is already a growth driver in an otherwise flagging economy. While traditional industries shrank by up to 3.6% from 2008 through 2011 in Europe, data-intensive sectors – where the use of digital identity is a key component of business – thrived with annual growth rates between 15% (e-commerce) and up to 100% (Web 2.0 communities).

- All told, the value created through digital identity can be massive – at a 22% annual growth rate, applying personal data can deliver a €330 billion annual economic benefit for organisations in Europe by 2020.

- Individuals will benefit to an even greater degree, as the consumer value will be more than twice as large: €670 billion by 2020. The combined total digital identity value could amount to roughly 8% of the EU-27 GDP.

- However, two-thirds of potential value generation – €440 billion in 2020 – is at risk if stakeholders fail to establish a trusted flow of data.

- Digital identity is relevant not just to Web 2.0 companies, but to the economy as a whole. The public sector and health care industry stand to profit most from personal data applications and are expected to realise 40% of the total organisational benefit.

- While the retail and Internet sectors already extensively use personal data, other sectors like traditional production and the aforementioned public services are in the infancy of digital identity value generation.

- Consumer concern has grown along with the increased use of personal data. 88% of people who are online consider at least one industry a threat to their privacy. Yet consumer research conducted for this study shows that stated concerns by individuals do not necessarily result in behavioural change.

- Most consumers have little idea what happens to their data. Only 30% have a relatively comprehensive understanding of which sectors are collecting and using their information. Individuals with higher-than-average awareness of data uses require 26% more benefit in return for sharing their data.

- Few individuals are in control of their digital identity. Just 10% of respondents had ever done six or more out of eight common privacy-protecting activities (e.g., private browsing, disabling cookies, opt-in/out). However, consumers who are able to manage and protect their privacy are up to 52% more willing to share information than those who aren't – presumably because they can adapt their data sharing to their individual preferences.

- Trust differs per sector: Consumers are on average 30% more willing to share data with e-commerce companies, cable operators and automobile manufacturers than with Web 2.0 communities.

- The "right to be forgotten" has a small but consistently positive impact on the willingness to share, increasing it by 10% to 18%.

- The preferred form of consent strongly depends on the type of data: Opt-out is considered adequate for less sensitive data by 69% of respondents, while opt-in is required for highly sensitive data by more than 80%. The issue of consent highlights a key dilemma: Control is important to consumers (82%), but so is convenience (63%).

- Overall, given proper privacy controls and sufficient benefits, most consumers are willing to share their personal data with public- and private-sector organisations. They want to spend their new currency on deals that they like.

- To unlock value, organisations need to make the benefits of digital identity applications very clear to consumers. Further, they need to embrace the new digital identity paradigm of responsibility, transparency and user control.

- Privacy is increasingly becoming an area of competition for organisations, which can differentiate themselves by providing the right privacy controls and privacy-by-default product design. Indeed, such a scenario may well play out in the desktop and mobile Web browsing market.

- Policy makers and regulators need to ensure adequate privacy safeguards and maintain a flexible approach that will encourage new applications and allow consumers to make their own informed choices on the extent to which they wish to generate value from their digital identity.

- Political intervention must account for shifting levels of acceptance regarding digital identity applications and the developments in the global marketplace. Failure to do so may hamper innovation as well as the competitiveness of domestic industries. Finding the right balance can spur local investment in digital identity applications and also attract industries to European markets that provide a safe haven for personal data.

executive summary

EXECUTIVE SUMMARY

"Digital identity": A driver of growth, a consumer hazard or both?

Increasingly, we are living double lives. There is our physical, everyday existence – and there is our digital identity. Most of us are likely more familiar with that first life than with the second, but as the bits of data about us grow and combine in the digital world – data on who we are, our history, our interests – a surprisingly complete picture of us emerges. What might also be surprising for most consumers is just how accurate and traceable that picture is.

In this report, we introduce the concept of digital identity – the sum of all digitally available information about an individual. How exactly digital identity develops is a massive concern for consumers and companies alike. Individuals are worried about losing their privacy and seeing their personal data used against them – for instance by insurers or employers discriminating against them based on personal data floating around the Internet. Companies, on the other hand, fear the backlash of approaching digital identity the wrong way, be it through their own applications or third-party applications that run on their networks, platforms or channels.

At the same time, the volume of data that is available, collected and analysed is growing rapidly, thanks to ubiquitous connectivity, vast increases in processing power and the growth of new sources like social media, online transactions, in-product sensors and digital media. The ability to put this data to good use – not the uses consumers fear but ones that can benefit them – is growing, too.

Views on digital identity tend to take one of two extremes: Let organisations do what they need to in order to realise the economic potential of "Big Data," or create powerful safeguards to keep private information private. But digital identity can't be cast in such black-and-white terms. While consumers voice concern about the use of their data, their behaviours – and their responses to a survey conducted specifically for this report – demonstrate that they are willing, even eager, to share information when they get an appropriate benefit in return. Indeed, as European Commissioner for Justice Viviane Reding remarked, "Personal data is in today's world the currency of the digital market. And like any currency it has to be stable and it has to be trustworthy."[1] This is a crucial point. Consumers will "spend" their personal data when the deals – and the conditions – are right. The biggest challenge for all stakeholders is how to establish a trusted flow of this data.

This study aims to reshape the discussion. To give business and political leaders a better understanding of this new phenomenon, it quantifies, for the first time, the current and potential economic value of digital identity across the economy as a whole and explores how consumers really view their personal data. An innovative survey of 3,000 individuals in Europe looked at their actual decision making, drilling down on the factors that spur, and hinder, the sharing of data. As a result, we were able to develop a new paradigm for unlocking the value of digital identity in a sustainable, consumer-centred way. These tools and insights, we hope, will contribute to the development of digital identity applications and policies that strike the right balance – and keep the data flowing.

[1] In January 2012 at the presentation of the proposal for a new General Data Protection Regulation

Digital identity can drive massive growth in an otherwise stagnant European economy

Taking a macroeconomic perspective, it becomes clear that digital data is already a growth driver in an otherwise flagging economy. These have not been the golden years for the traditional production, retail, financial services and telecommunication and media sectors, which saw compound annual growth rates (CAGR) of 0% to -3.6% from 2008 through 2011 in Europe. Data-intense sectors, on the other hand, where the use of digital identity is a key component of business, performed strongly over the same period: Web 2.0 communities saw an annual revenue growth of about 100%, while the e-commerce sector had a CAGR of 15% and the online information and entertainment sector of 22%.[2]

In an overall stagnant European economy, the applications built on the use of digital identity can drive massive value growth for both public- and private-sector organisations: At a 22% annual growth rate, the annual economic benefit can reach €330 billion by 2020.

Those applications can help tackle some of society's most pressing problems, too. In the health care sector, data-driven applications like personalised medicine, decision support systems and electronic records shared among providers can improve quality and efficiency of care – particularly important goals given Europe's ageing population. In the public sector, personal data-driven initiatives to fight tax evasion and citizen self-service portals, where tasks like driving license renewals can be performed online, can increase tax revenues and lower spending, giving governments some relief from the budget pressure they are under.

It is important to realise that, although the public debate on monetisation of personal data is dominated by the perspective on Web 2.0 players, digital identity is relevant, and important, for the whole economy.

It is important to realise that, although the public debate on monetisation of personal data is dominated by the perspective on Web 2.0 players and the digital economy, digital identity is not just the realm of the Facebooks and Googles of the world. It is relevant, and important, for the whole economy. In fact, it is the public sector and health care that stand to profit the most from personal data applications – potentially realising 40% of the total organisational benefit.

The benefits of digital identity are relevant and important for consumers as well. Indeed, BCG estimates that the consumer benefit will be more than double the organisational value – €670 billion a year by 2020 – mainly stemming from reduced prices (passed on by companies seeing data-driven cost savings), the time savings that self-service transactions will bring and the high value individuals place on free online services, supported at least in part by the use of personal data.

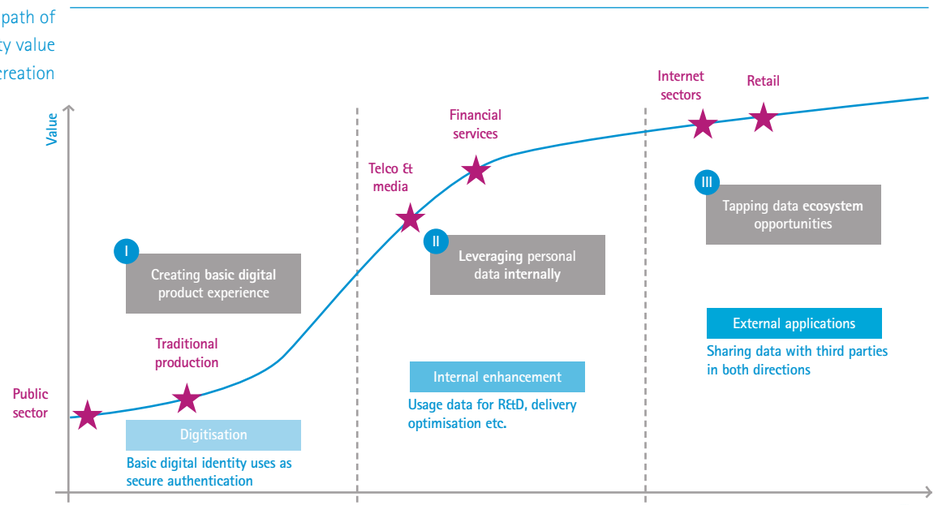
Sectors are at different stages of generating value from personal data

Eight sectors collectively cover the whole economy, but individually face very different conditions and challenges in applying digital identity: traditional production, retail, financial services, telecommunications and media, public services/health, Web 2.0 communities, e-commerce and online info/entertainment.

[2] Eurostat; BVH; comScore; BCG analysis

EXECUTIVE SUMMARY

Evolutionary path of digital identity value creation



Digital identity intensity

Each of these sectors is at a very different stage of unlocking value through personal data applications.

Retail and the three Internet sectors are already at a relatively advanced level; these organisations routinely leverage personal data internally for R&D to optimise the delivery of their goods and services and for other purposes. They often tap into the wider ecosystem of data-related opportunities as well, such as sharing – and selling – information to third parties.

Companies in the telecommunications and media sector, including cable operators, have access to a vast amount of personal data in principle – mainly relating to telephony and Internet usage or TV viewing – but so far make relatively little use of it. While customer self-service and process automation are currently the major applications of digital identity, we expect the focus to shift to innovative new services and enhanced user experience.

The traditional production and public sectors, meanwhile, are at the very beginning of the path. Many of these organisations are only now starting to create a basic digital product experience or to embrace digitisation – such as government agencies and health care providers migrating to electronic records and setting up processes that leverage this data along the value chain.

The volume – and variety – of data is expanding

The economic growth prospects for digital identity are fuelled by two important factors: First, there is the exponentially expanding amount of available data, which is expected to grow by 45% per year through 2015, to roughly 7 zettabytes. To put that in perspective, that is more than 1,000 gigabytes of data – twice the capacity of a standard laptop – of data for every person on earth in 2015. Second, there is the rapidly improving ability to process and analyse that data. The "data explosion" is driven by global trends resulting not only in increased volume, but also completely new types of data.

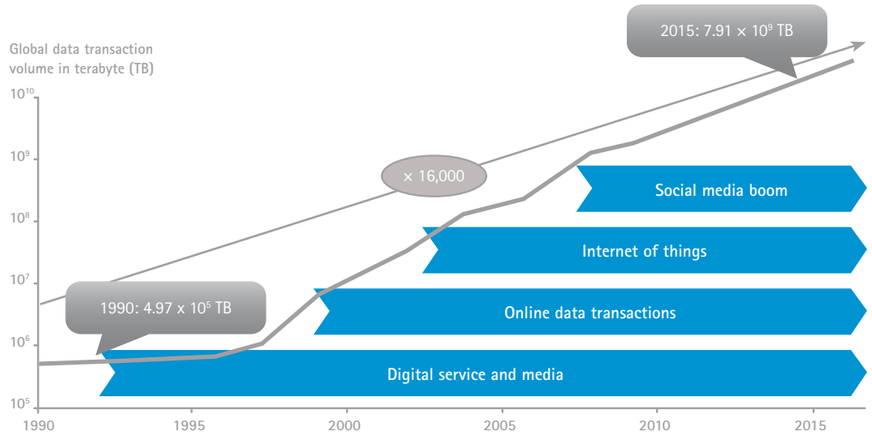
The "data explosion" is driven by global trends resulting not only in increased volume, but also completely new types of data.

The social media boom is perhaps the most important of these trends, as it has allowed formerly passive data subjects to actively share and distribute information on a large scale. By 2015, one quarter of the world's population will be a member of a social network and will to some extent share personal information, including demographical data, likes and preferences, images, video and even location data.[3]

The other trend leading to increased data variety is the "Internet of things." In-product sensors that can "call home" via the Internet and relay usage data are becoming increasingly prevalent. Automobiles, home appliances and energy meters are among the traditional product categories that have – or soon will have – integrated links to the Internet. Not including phones or PCs, we expect to see an additional 75 million devices with direct connections to the Internet in Europe by 2015.[4]

For both organisations and consumers, this increased data volume has the potential to create significant value, which will manifest itself in a variety of ways. By creating more personalised products – and lever-

Global data explosion



Source: comScore; Facebook; Sandvine: "Information White Paper," 2011; Sandvine: "Digital Contents White Paper," 2010; METI E-Commerce survey; IDC; consumer research; BCG analysis

[3] Source: Morgan Stanley; Strategy Analytics; eMarketer; UN "World Population Forecast"; BCG analysis

[4] Source: ABI; Berg Insight; IDC; Yankee Group; Gartner; Analysys Mason; BCG analysis

EXECUTIVE SUMMARY

aging data to enhance existing products – businesses can create new revenue streams and expand old ones. Research and development can be improved, meaning more relevant and more attractive products – which benefit all sides.

The six key trends in digital identity applications

While the actual applications of personal information vary from sector to sector, and even from organisation to organisation, they invariably fall into one of six categories. These are the megatrends of digital identity:

- **Process automation.** By integrating personal data into their processes, organisations can automate – and simplify and speed up – transactions that traditionally required users to identify themselves, express their preferences or perform some kind of manual action. For example, the Oyster Card carried by London commuters authenticates them when they board buses and trains, automating ticketing and access control.

- **User enablement.** Digital identity gives individuals the ability to perform transactions autonomously, without any human assistance. Customer self-service is a prime example. It continues to grow strongly in sectors where it has been applied for decades and is being introduced in more and more new industries. Denmark, for example, has one of the most advanced e-government programmes in the world and generates €200 million in annual savings with electronic invoicing alone.

- **Personalisation.** Customising products and services to a particular individual's preferences and needs makes them more relevant to that person. That spurs sales for the organisation and satisfaction for the consumer. Traditionally, personalised products came about through bespoke solutions at high cost premiums and for small target audiences. Digital identity enables personalisation on a wide-scale, cost-effective basis. Amazon's dynamically generated recommendations – based on a user's purchasing and browsing history – are estimated to generate some 25% of the e-commerce giant's sales.

- **Enhanced delivery.** The availability of both more volume and more types of data enables organisations to increasingly extract operational insight from it. This allows them to improve the delivery of goods and services. For instance, IBM and the U.S. insurer Wellpoint are developing a system to analyse huge volumes of data from many sources – including research papers, medical textbooks and population health data – to detect diseases and suggest treatment options. Such solutions can lead to many more patients benefiting from optimal care.

- **Personal data-driven R&D.** Using a range of data sources – such as product reviews, comments posted on social media sites and usage data from in-product sensors – companies can also gain insights that let them better focus their research efforts and shorten development cycles. This trend has already been adopted by major consumer goods companies, including Procter & Gamble, whose Vocalpoint P&G community gets customers more deeply involved in the development and testing of new products.

- **Secondary monetisation.** The data that an organisation holds, or the insight derived from it, is valuable to other parties – valuable enough that selling it can open up a significant new revenue stream. The online sectors pioneered the secondary monetisation of personal information, but it is a trend taking hold – and rapidly – in other sectors as well. Even the public sector has benefitted from putting its data up for bids: In the United States, the state of Florida took in more than $60 million in 2010 by selling information it collects from drivers.

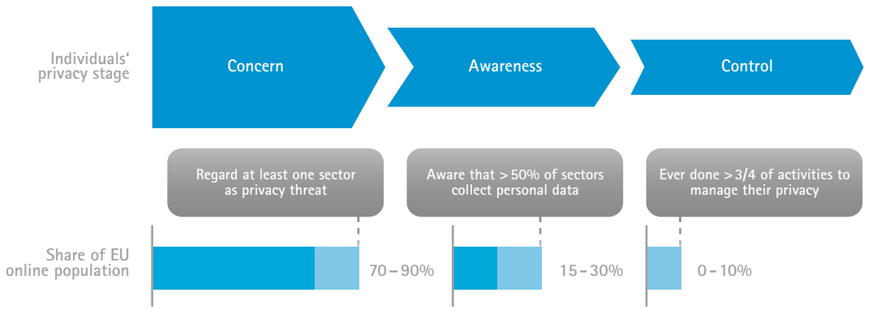
Personal data uses concern most individuals, few are fully aware and in control of them

Along with use of personal data, the concerns of people have also grown. The majority of individuals have concerns about the use of personal data by companies. A major Europe-wide study, Eurobarometer[5], put the figure at 70%, while BCG's own representative survey of more than 3,000 European consumers, conducted for this report in August 2012, revealed that 88% of people who are online consider at least one industry or sector a threat to their privacy.[6]

High as these numbers are, they are hardly surprising considering the high-profile data breaches of recent years. When Sony's PlayStation Network was breached in April 2011, it didn't just result in a few user accounts being compromised. Personally identifiable information of 77 million subscribers was stolen – a breach so significant that the entire service was shut down for 24 days and Sony incurred direct costs associated with the incident of ¥14 billion, or roughly €128 million.[7]

Incidents like these also heighten consumers' more subjective fears that new technologies like RFID, face recognition and user profiling will unravel the anonymity and privacy they have long enjoyed – or at least thought they enjoyed. Data collection and use is rarely transparent to users. Indeed, while the BCG survey found that most individuals are concerned about their personal information, far fewer realise the extent to which organisations acquire and leverage it. Only 30% of respondents had a relatively comprehensive understanding of which sectors were collecting and using their information.

Share of concern, awareness and control



Source: BCG digital identity survey (n = 3,107, August 2012)

[5] Special Eurobarometer 359, field work conducted 2010, published 2011

[6] BCG digital identity survey (n = 3,107, August 2012)

[7] Sony's script of revisions to reporting of fiscal year 2011 published on 23 May 2011

EXECUTIVE SUMMARY

Fewer individuals still are both aware of data use and able to exert some control over it. When we asked respondents how many of eight common privacy-protecting activities they had ever performed – actions like changing the privacy setting in a social network service, or surfing the Web in "private" mode – just 10% said they had ever done six or more of these things. Part of the explanation, of course, is that many data-collecting organisations do not offer any options or settings enabling users to manage their privacy.

While few consumers are fully aware of how their data is being used and even fewer are capable of actively managing it, most individuals expect their digital identity to be treated responsibly and openly: 79%, for example, said companies should be more transparent about use of personal data.

Leveraging digital identity means understanding how consumers really view it

As the whole topic is centred around the individual, it is vital to understand how consumers really view and are willing to use their digital identity. Past research into the use of personal data has mainly focussed on consumer attitudes, asking people about their concerns and opinions. But as this report demonstrates, individuals' privacy concerns and their behaviour don't always match up. To home in on actual behaviour and provide a quantitative perspective on individuals' willingness to share personal data, we applied a value-based methodology for this study's survey.[8]

User controls increase consumers' willingness to share data

Our research indicates that the level of anxiety consumers express regarding their privacy is not a strong indicator of their actual data-sharing behaviour. Different groups of consumers expressed very different levels of concern. Some were concerned about the data use of just one, or none, of the covered sectors; others were concerned by all or nearly all of them. But we found that their actual privacy valuation did not differ. Privacy, it seems, is comparable to climate change: Stated concerns by individuals do not necessarily result in a change in behaviour in their day-to-day lives.

Different groups of consumers expressed very different levels of concern. But we found that their actual privacy valuation did not differ.

However, other factors do significantly influence a consumer's willingness to share data:

- **Awareness.** Consumers with higher awareness of data uses require higher benefits in return for sharing their data. Specifically, those with higher-than-average awareness require 26% more benefit in return for sharing their data. The currently low degree of awareness thus represents a real risk for organisations seeking to create value via digital identity – especially if they conduct practices that consumers would not knowingly approve of.

- **Control.** Having easy-to-use privacy controls and sharing options can substantially increase a consumer's willingness to share personal data. BCG's survey found that consumers who are able to manage and protect their privacy (through common actions such as changing privacy settings in a social network or opting out of certain data uses) are up to 52% more willing to share information than those who aren't.

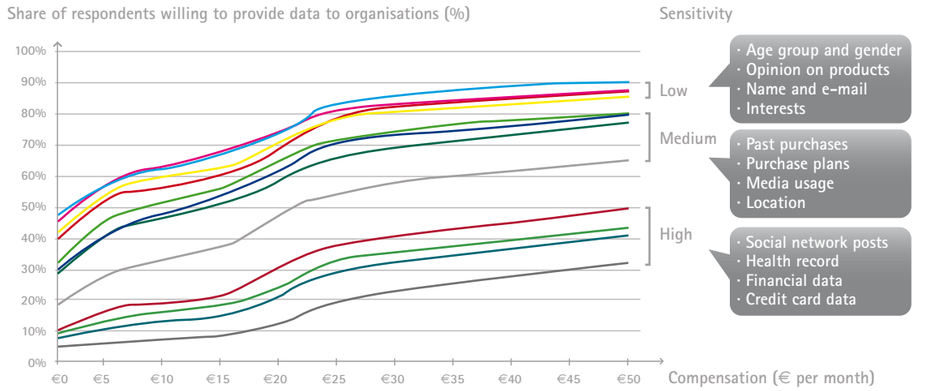
Consumers who are able to manage and protect their privacy are up to 52% more willing to share information than those who aren't.

Ease of use is also critical: For low- and medium-sensitivity data, the easier consumers perceived those controls to be, the more they shared. For sharing age and gender information, for example, individuals who had a relatively easy time managing their privacy were 37% more willing to share than those who had a relatively difficult time.

- **Data types, sectors, collection methods and uses.** Consumers also make clear distinctions between different types of data, industry sectors, collection methods and the uses to which data is put. Their level of trust differs depending on the sector, for example: Consumers, we saw, are on average nearly 30% more willing to share with e-commerce companies, cable operators and automobile manufacturers than with Web 2.0 communities.

Exhibit *Sensitivities of data types* shows how consumers differentiate between data types. While low-sensitivity information is shared by more than 40% of people even without receiving a direct benefit, most individuals are unwilling to part with highly sensitive data even for large rewards. It should be noted that the research method we applied provides very meaningful data on the relative differences, but the absolute monetary

Sensitivities of data types



Source: BCG digital identity survey (n = 3,107, August 2012)

[8] Conjoint methodology is a technique BCG frequently utilises in project work to identify how several dimensions of a product influence consumer decisions (for example, how design, brand, environmental impact and price affect the decision to buy an automobile).

EXECUTIVE SUMMARY

figures cannot be interpreted as the actual "value of the data." They rather serve as indications of the value consumers place on their personal information.

"The right to be forgotten" has a small but positive impact on sharing

The study's research also shed some light on how some of the privacy rights and controls in the proposed General Data Protection Regulation are viewed by consumers:

- **The right to be forgotten.** This has a small but consistently positive impact on the willingness of individuals to share private data. When respondents were given the right to have their data deleted at their request – as opposed to deletion being outside their control – they were 10% to 18% more willing to share information. This effect was most pronounced for people who had not shared private information with organisations before – or at least, thought they hadn't.

- **Consent.** The form of consent consumers prefer strongly depends on the type of data at issue. For some types of less sensitive data, for example, up to 69% of respondents considered opt-out, or even assumed consent, appropriate. For highly sensitive data, in contrast, more than 80% of respondents said an opt-in mechanism was a must.

With regard to consent, the survey also highlights a key dilemma digital identity poses. Most respondents (82%) expressed the wish to decide whether to allow data use in each instance. However, a majority (63%) also agreed with the statement "I do not like it when a website asks me for the same information every time I open it." Control is important to consumers – but so is convenience. Balancing these often conflicting aims will be tricky but critical.

Yet perhaps the most important takeaway from this study's research is this: Consumers want to share their data – if the benefits and the privacy controls are right.

Yet perhaps the most important takeaway from this study's research is this: Consumers want to share their data – if the benefits and the privacy controls are right.

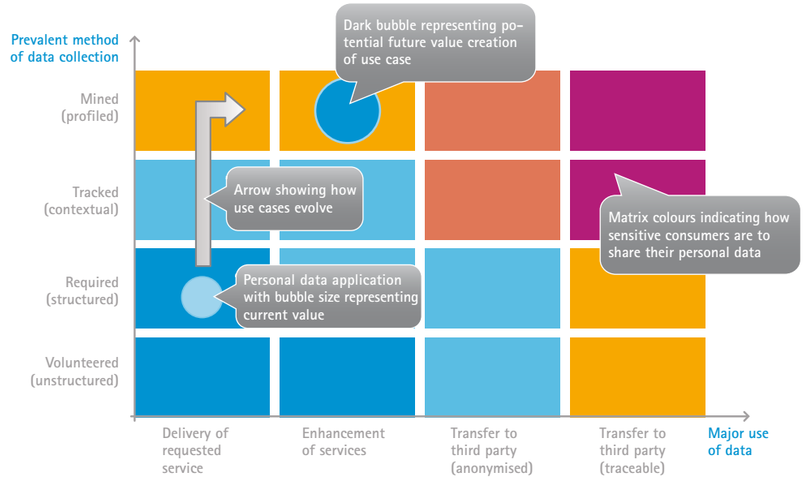
A framework for analysing acceptance of digital identity applications

While the applications vary, a common framework can be used to evaluate every use case. This framework focuses on the two key dimensions in how digital identity is leveraged: the method of data collection and the manner in which it is used. Consumers consider these same two dimensions when viewing the trade-off between the value and cost of sharing information.

Indeed, their willingness to share declines as the methods for collection and use move toward the outer boundaries, where consumers feel they have less control over the collection and use of their data; for example, when organisations acquire data through tracking or data mining, or when they allow third parties to access it. Thus, consumer sensitivities can also be plotted on the same framework, and we can see at a glance both the opportunity and the risk any single application presents.

Another lens through which to look at applications is the traceability and completeness of the personal data that is used. Individuals typically prefer that businesses use digital identities that are incomplete and not traceable – data that may provide insight on usage or purchasing patterns, for example, but can't be linked back to a particular person. Organisations, on the other hand, generally prefer to use complete and traceable digital identities, as the granularity in the data and the ability to address specific consumers represent greater value. Between these two poles, however, is space for compromise: solutions that balance privacy with value generation. For example, if control schemes guaranteed that digital identities remained untraceable, more complete identities could be used. Likewise, if data collection was limited to less complete information, more traceable digital identities could be employed. Just as organisations need to understand the impact of their collection and use methods, they must carefully assess the levels of traceability and completeness to be used in their applications and business models. In this context, it is interesting to observe that the level of acceptance of data-intense applications can vary greatly between sectors, and even between organisations within the same sector.

Digital identity framework



So while one company might run into no problems collecting a user's location data and transferring it to a third party, another company might do the same thing and face tremendous consumer backlash. The difference in consumer acceptance can often be explained in terms of

The level of acceptance of data-intense applications can vary greatly between sectors, and even between organisations within the same sector.

EXECUTIVE SUMMARY

brand awareness and loyalty, the "cool" factor of a given product or application or the significant consumer surplus associated in particular with "freemium" services.

Towards a new paradigm for digital identity

As detailed above, the opportunities digital identity presents – when managed carefully – are enormous. But so, too, are the lost opportunities, should it not be handled in a thoughtful, balanced way. BCG estimates that two-thirds of the potential value generation – or €440 billion in 2020 alone – is at risk if stakeholders fail to establish a trusted flow of personal data.

BCG estimates that two-thirds of the potential value generation – or €440 billion in 2020 alone – is at risk if stakeholders fail to establish a trusted flow of personal data.

To unlock the full value, organisations need to make the benefits of digital identity applications very clear to consumers. Just as importantly, they need to embrace the new digital identity paradigm: It starts with responsibility. Then it adds transparency to limit the risks presented by hidden practices that, once uncovered, become the focal point of a public firestorm.

Organisations need to communicate and be open about how exactly they acquire and use data. Finally, there must be user control. As evidenced by the consumer survey data we present, individuals' preferences regarding privacy and data sharing differ – and differ widely. Giving them options and controls might reduce sharing for specific individuals in specific situations, but overall it will likely increase the sharing of personal data.

To help organisations successfully adopt the new paradigm, we offer the following recommendations:

- **Engage customers for sustainable personal data usage.** Organisations should involve and educate consumers on personal data applications, as well as on privacy management. And they should do so in a carefully thought-out, well-structured way. As we show in this report, three elements are essential to ensure a sustainable flow of data: First, the benefit a consumer receives has to exceed the "cost" of sharing the data. Second, there needs to be transparency on how the data is used. While this might initially reduce sharing, it limits the risk of brand damage and helps to attract more informed customers. Third, privacy controls should be available and easy to use. They will significantly increase data sharing by individuals, likely offsetting any negative impact on sharing resulting from increased transparency.

- **Take accountability for a trusted flow of data.** Every business and public agency that depends on digital identity applications should define guiding principles for how it works with personal data. These principles should be communicated clearly both within and outside the organisation to ensure unmistakable accountability and commitment. At the same time, an organisational structure and processes that hardwire compliance with those principles should be established.

- **Increase data security in order to safeguard digital identity.** As the examples in this report demonstrate, data breaches cause damage on multiple fronts: Consumers see their personal information compromised; organisations see trust erode and their brand and reputation suffer. There are the direct costs, as well, to both consumer and organisation: The level of security – not just technical measures, but also policies and access control – needs to reflect the high value of personal data.

- **Build a data-driven organisation, not just a data-driven IT department.** Consumers aren't the only ones who benefit from transparency. Organisations do, too. They should know what data is available both inside and outside their own walls, and all parts of the organisation should be encouraged to identify value creation opportunities, experiment with new applications and develop analytical talent.

Striking the right balance in policy and regulation

Across Europe, policy makers are actively discussing proposed rules on privacy. While safeguards are needed, the regulations that ultimately result should be flexible enough that consumers can make their own informed choices about whether and how they share data. Individuals should be able to generate value from their digital identity – if they wish to do so. At the same time, they should be able to rest assured that their data isn't being put to unintended or undesired purposes.

Once again, balance is key. Privacy protections shouldn't be so stringent that they discourage innovation, nor should they be so weak that they enable misuse. It also requires sometimes taking a step back from some of the emotion that can imbue discussions on privacy. Politicised and hyped concerns about the privacy implications of new applications – concerns voiced recently in the case of Google's "Street View" feature – can morph into widespread outcry as it did in Germany.[9] That, in turn, could trigger blanket prohibitions on certain data uses – which might impact a wide range of applications beyond the targeted application. Ultimately, such prohibitions designed to protect individuals can actually hamper or delay innovations that would benefit them and can put domestic industries at a competitive disadvantage relative to their international competition. Balance means, too, that sometimes a "highest" level of protection that stalls novel new applications is less desirable than a "high" level that spurs them.

While safeguards are needed, the regulations that ultimately result should be flexible enough that consumers can make their own informed choices about whether and how they share data.

The most successful policies will put the consumer front and centre, but also enable experimentation in, and the development of, new uses of personal data. They will be firm regarding principles, but allow for flexibility in implementation and enforcement. They will give organisations a certain amount of leeway, acknowledging that different markets and regions have different historical, cultural and political legacies – and different, constantly shifting attitudes towards privacy and new uses of personal data. A balanced approach, both in policy and in the applications themselves, is essential if we are to realise the enormous benefits digital identity has to offer.

[9] Spiegel Online, "Die Foto-Hysterie verdeckt echte Datenschutz-Probleme," 3 November 2010

part 1

DIGITAL IDENTITY: A DRIVER OF GROWTH, A CONSUMER HAZARD OR BOTH?

A CONSUMER HAZARD OR BOTH? A DRIVER OF GROWTH,

DIGITAL IDENTITY – A DRIVER OF GROWTH, A CONSUMER HAZARD OR BOTH?

By now, we have all heard the analogies highlighting the importance – and value – of data. It is the new gold. The "new raw material of the 21st century," as Francis Maude, the UK Minister for the Cabinet Office, put it.[1] Whatever the label, the basic message is the same: Data is an untapped resource of vast potential that only needs to be unearthed and refined before the riches roll in.

If only.

For while the analogies make for catchy wordplay, they all have the same flaw: Data is still a big unknown. It is valuable, of course – but how will that value be realised? What types of applications and innovation can data enable – and what will they bring? What challenges lie in the path, and how can those obstacles be overcome? These are questions that are only starting to be answered. And they are questions that become even more important – and more difficult to answer – when the data in question is personal information.

Individuals today enjoy a kind of dual citizenship: We have our normal, everyday lives in the physical world, but we also have our digital identity – all the bits and pieces of information about us that are readily, and increasingly, available in digital form; data that is collected and analysed to create a surprisingly accurate, and ever-improving, picture of who we are, what we do, what we like (and what we dislike, too).

Organisations understand that there is particular value to be found in digital identity. Online businesses, for example, regularly use a consumer's purchasing history and preferences to recommend new products or to target their marketing efforts. But digital identity – and its benefits – is relevant to the entire economy. Indeed, its applications can help solve some of society's most pressing problems. In health care, personalised medicine, decision support systems and electronic records that can easily be exchanged between doctors, hospitals and labs can improve quality of care – and even prolong lives. In the public sector, data-driven initiatives to fight tax evasion and create citizen self-service portals (where transactions can be performed online instead of in offices) can increase tax revenues and lower costs – easing the budget pressure almost all European governments now face.

The value that can be derived from digital identity applications is potentially enormous, and can be a significant force in spurring an otherwise stagnant European economy.

All told, the value that can be derived from digital identity applications is potentially enormous, and can be a significant force in spurring an otherwise stagnant European economy. BCG estimates that at a 22% annual growth rate, the annual economic benefit for private- and public-sector organisations can reach €330 billion by 2020.

[1] The Guardian, 18 April 2012

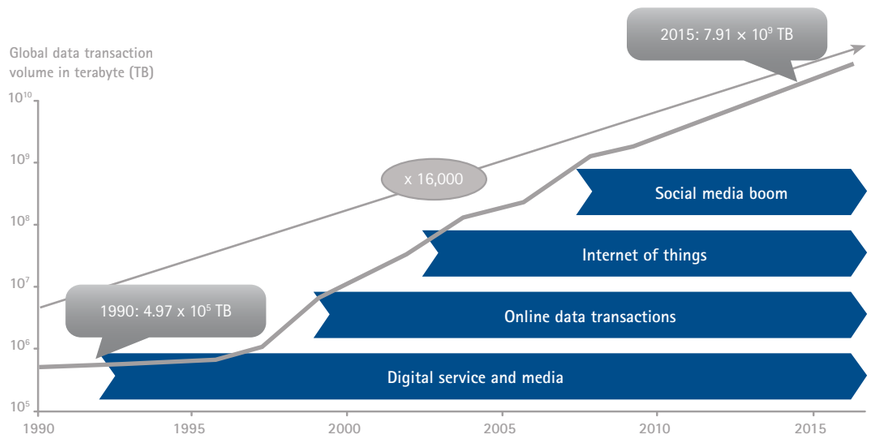
Consumers benefit in a host of ways, too. They save time through automated transactions. They save money when the efficiencies businesses reap are passed down in the form of lower prices. And they place an especially large value on the free online services that are supported, at least in part, by the use of personal data – enough that consumers are willing to divulge pieces of that data in return for using Facebook, Google and other services. As European Commissioner for Justice Viviane Reding said in January 2012, when presenting the proposal for the new General Data Protection Regulation, "Personal data is in today's world the currency of the digital market."

Currency, however, can be volatile, and personal data is no exception. Data breaches and fears about data misuse are giving consumers pause. They are concerned about their privacy and what happens to their data once it is in a third party's hands. If consumers hold back their personal information, the value potential of digital identity will be held back as well. "Like any currency, [personal data] has to be stable and it has to be trustworthy," Reding went on to say. For business leaders – and policy makers now discussing possible data privacy protections – the challenge is to establish the trust that keeps the currency flowing.

For business leaders and policy makers the challenge is to establish the trust that keeps the currency flowing.

The discussion on digital identity has tended to pit two ideas against each other: What is the potential economic value of personal data? How can consumers be protected from its misuse? What it needs to do, instead, is balance these two goals, creating applications and policies that

Global data explosion



Source: comScore; Facebook; Sandvine: "Information White Paper," 2011; Sandvine: "Digital Contents White Paper," 2010; METI E-Commerce survey; IDC; consumer research; BCG analysis

A CONSUMER HAZARD A DRIVER OF GROWTH, OR BOTH?

spur innovation – and value – while safeguarding privacy. That means taking a close, critical look at both the potential of digital identity and consumer sensitivities. The insight that results will drive flexible solutions that will shape our future.

As the volume and variety of data grows, so does its value

Gold may be a scarce natural resource, but digital data is the opposite: It is readily available and rapidly increasing at an exponential rate. BCG expects that the global data transaction volume will grow at 45% annually through 2015, to 7.91 × 10^3 terabytes, or approximately 7 zettabytes. To put that in perspective, that is enough data to fill the hard discs of two standard laptops for every person on earth in 2015.

The explosive growth of digital data is a phenomenon that both consumers and organisations are very familiar with. A decade ago, a consumer in Europe could buy a 64-megabyte memory card – capable of storing three minutes of high-definition video – for about €20. Today for that price, she could buy a 32-gigabyte card capable of storing some 25 hours of HD content.

But where the data is flowing from is the more interesting part of the story. The flood of digital data is coming to a large extent from new and even unexpected places – sources that are particularly rich in the personal information that, collected, aggregated and analysed, extends our digital identities.

The "data explosion" is being driven, specifically, by four global trends:

- **Social media boom.** These online services – including Facebook, Twitter, VK, LinkedIn and XING – let users not only interact with each other, but also share news and information, including demographical data, likes and preferences, images, video clips and even location data (where they are and what they are doing there). While these services often come under scrutiny for their privacy practices, the best known continue to see their ranks swell: Already, Facebook has 1 billion users worldwide, and by 2015, one quarter of the world's population will be a member of a social network.[2]

- **The Internet of things.** In-product sensors that can "call home" via the Internet and relay usage data are becoming increasingly prevalent. Automobiles, home appliances and energy meters are among the traditional product categories that have – or soon will have – integrated links to the Internet. Not including phones or PCs, we expect to see an additional 75 million devices with direct connections to the Internet in Europe by 2015.[3] Potentially hundreds of millions more will be equipped with near-field communication chipsets that allow them to connect to the Internet through other devices.

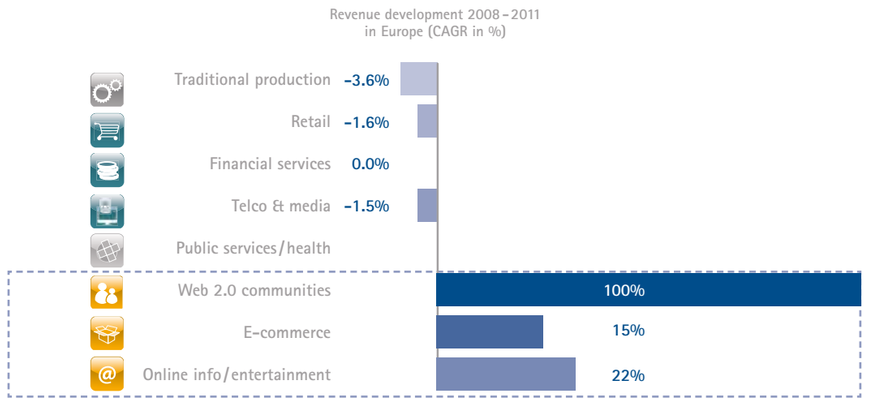
- **Online data transactions.** Each time a transaction occurs online – a song purchase, an airline seat upgrade, a payment of an electricity bill – data is collected, stored and made available for later use. Even transactions that are ultimately abandoned – like the £1.02 billion worth of goods UK consumers put in their online shopping carts in 2011 but never purchased – are captured.[4]

- **Digital services and media.** Faster, more prevalent Internet access, low-priced storage media and the growth of mobile devices have resulted in a vast increase in the amount of digital multimedia consumed by users through services like YouTube or Spotify. The shift to digital is exemplified by Netflix, the popular US video service that delivers titles by DVD and online streaming, which saw a 72% increase in the number of customers who utilise streaming only in 2011.[5]

From a macroeconomic perspective, it is clear that the digital data explosion can fuel economic growth. It is no secret that growth has been elusive for traditional business sectors in Europe. Between 2008 and 2011, the financial services sector saw revenues remain flat, while the retail industry had a compound annual growth rate (CAGR) of -1.6% and the traditional production sector a CAGR of -3.6%. Yet over the same period, highly data-intense industries thrived. The e-commerce industry enjoyed a CAGR of nearly 15%, and for Web 2.0 communities – the Facebooks and LinkedIns of the world – the rate was just over 100%. Within the Internet sector, revenue has been closely tied to the use of personal data: On social networking sites, advertising is targeted to users' profiles and posts; on e-commerce and digital media sites, personalised recommendations drive usage and sales.

From a macroeconomic perspective, it is clear that the digital data explosion can fuel economic growth.

Sector growth



Source: Eurostat; BVH; comScore; BCG analysis

[2] Source: Morgan Stanley; Strategy Analytics; eMarketer; UN "World Population Forecast"; BCG analysis

[3] Source: ABI; Berg Insight; IDC; Yankee Group; Gartner; Analysys Mason; BCG analysis

[4] Research commissioned by Experian, published 19 March 2012

[5] Interpret, 7 March 2012

A CONSUMER HAZARD OR A DRIVER OF GROWTH?

None of this has escaped the attention of traditional businesses, who are starting to ramp up their own efforts to leverage digital identity. Among the more prominent examples:

- **Personalised automobile systems.** While many car manufacturers now routinely incorporate digital sensors in their automobiles – typically to monitor vehicle systems to enhance performance and troubleshoot problems – some are going a step further, integrating sensors with personalised services. The result: new subscription-based revenue streams, or rejuvenated offerings that are more compelling to buyers. One initiative, BMW ConnectedDrive, integrates in-car satellite navigation – an option that, industry-wide, has lost ground to less expensive after-market GPS units – with safety, entertainment and Internet services. Users can search Google directly from their navigation unit or send a destination address to the system from Google Maps. This initiative enabled BMW to take a product that was facing commoditisation and differentiate it, keeping its sales healthy.

- **Social marketing campaigns.** Big brands are leveraging online social networks to improve their engagement – and boost their visibility – with consumers. Farmers Insurance, the third largest general insurer in the United States, teamed with Zygna, maker of the popular Facebook-based game FarmVille, to promote its brand. An in-game Farmers airship provided players with insurance to protect their FarmVille crops; clicking on the airship took players to the company's Facebook fan page. Before this campaign, Farmers had 6,500 Facebook fans. Ultimately, it had 2.4 million – all potential advocates for spreading the word about the company.[6]

- **Self-service apps and portals.** Telecommunications providers and financial services companies are moving more customer transactions from the offline labour-intense world to online self-service portals (e.g., My Vodafone). And for good reason: Online and mobile transactions are far less expensive to support. Indeed, for banks, they run just 5% of the cost of branch transactions.[7]

- **Actual behaviour-based insurance policies.** The emergence of mobile devices capable of transmitting location and usage data allows insurance companies to base their premiums on actual instead of predicted behaviour. Case in point: GMAC Insurance has pioneered a pay-as-you-drive (PAYD) car insurance policy in cooperation with GM. Customers can let their OnStar telematics system automatically transmit the mileage of their car and pay insurance premiums only for the miles actually driven.[8]

As the euro crisis puts pressures on government budgets, early adopters are showing how data-driven value creation can help ease the strain.

In the health care and public sectors, the potential benefits of digital identity applications may be especially compelling. As the euro crisis puts pressures on government budgets, early adopters are showing how data-driven value creation can help ease the strain. In Italy – which loses an estimated €120 billion each year to tax evasion – a system called "Redditometro" analyses some 100 indicators of a citizen's lifestyle to optimise tax audits. In 2011 alone, €11.5 billion was recovered.[9] In the health care sector, BCG estimates that insurers, providers and other organisations in the value chain can achieve overall cost savings of 10% to 20% by better leveraging personal data – no small benefit for an industry that has been seeing ever-growing cost increases, fuelled in large part by Europe's ageing population.

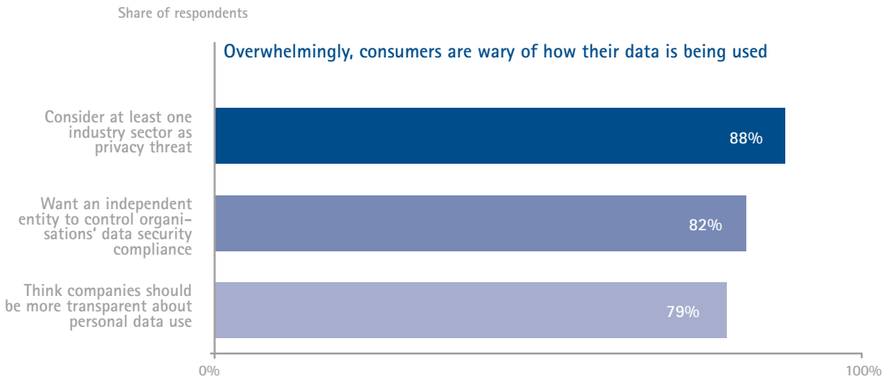
Digital identity enables businesses to better understand what their customers like, and want, to serve them more efficiently and to develop new and enhanced revenue streams. The benefits they achieve are passed down to consumers, as well, in the form of lower prices, time savings or new and valuable services. This isn't happening on a small scale. We estimate that digital identity applications can bring a quantifiable annual benefit of approximately €1 trillion in Europe by 2020.

Achieving this potential is by no means a given, however. Consumer sensitivities – heightened, as we will show, by an organisational approach to digital identity that largely ignores them – present a considerable risk; one that has to be understood, addressed and mitigated.

Consumer research reveals a deep lack of trust

The concerns and anxieties of consumers regarding the use of their personal data are mounting. Eurobarometer, a major Europe-wide study conducted in 2010, revealed that 70% of consumers were concerned about how companies were using their personal information.[10] BCG's own research study of more than 3,000 European consumers, conducted for this report in August 2012, not only confirmed the high level of concern, but demonstrated that, if anything, trust was eroding further. Nearly 90% of respondents considered at least one industry sector a threat to their privacy, 82% thought an independent entity should ensure the data security compliance of organisations and 79% thought companies should be more transparent about the use of personal data.

Consumers' concerns



[6] Neal Schaffer, October 2010; Farmers Insurance

[7] BCG analysis

[8] GMAC Insurance and General Motors websites

[9] The International Herald Tribune, 7 February 2012

[10] Special Eurobarometer 359, field work conducted 2010, published 2011

A CONSUMER HAZARD OR A DRIVER OF GROWTH?

Consumer concerns fall into two broad categories:

- **Actual damage:** These are the worries that stem from the real-world events – and real-world damage – that have increasingly filled the headlines in recent years. Data breaches by hackers or disgruntled employees have compromised personal information stored on corporate servers (names, mailing addresses, national insurance numbers, credit card information, e-mail addresses and so on) and led to credit card fraud, identity theft, spam and other illegal or undesirable consequences.

High-profile data breaches since 2011

RSA	March 2011	Up to 40 million employee records could have been stolen through spear-phishing attacks
epsilon	March 2011	E-mail addresses and names of millions of customers, several financial institutions (e.g., CitiGroup) and the non-profit organisation College Board were exposed
Sony	April 2011	A total of 77 million PlayStation Network accounts were hacked, exposing names, e-mail addresses and credit card data. Sony lost millions during the long downtime of the network
Travelodge	June 2011	The UK online travel provider's customer database was hacked, with its clients' e-mail addresses and names exposed
ESTsoft	July 2011	Malware attack on ESTsoft's servers led to exposure of the names, user IDs, hashed passwords, birthdates, genders, telephone numbers, and street and e-mail addresses of 35 million Koreans
Tricare/ SAIC	September 2011	A SAIC backup tape was stolen from a Tricare employee, containing medical and financial information of 5.1 million individuals; a $4.9 billion lawsuit followed
NASDAQ	October 2011	Attackers hacked a cloud-based NASDAQ system, which enabled them to monitor boardroom-level communications of more than 10,000 executives
Telefonica O_2	January 2012	During routine maintenance procedures, customers' phone numbers were logged to websites when they were accessing the service via 3G or WAP, exposing the data to website publishers
LinkedIn	June 2012	Files containing 6.4 million passwords were found on underground hacker websites by security specialists and are expected to belong to LinkedIn members
Philips	August 2012	Hackers targeted Philips' servers and obtained more than 200,000 e-mail addresses, along with customer information such as names, postal addresses, birthdays, passwords and phone numbers

Source: Press; company websites

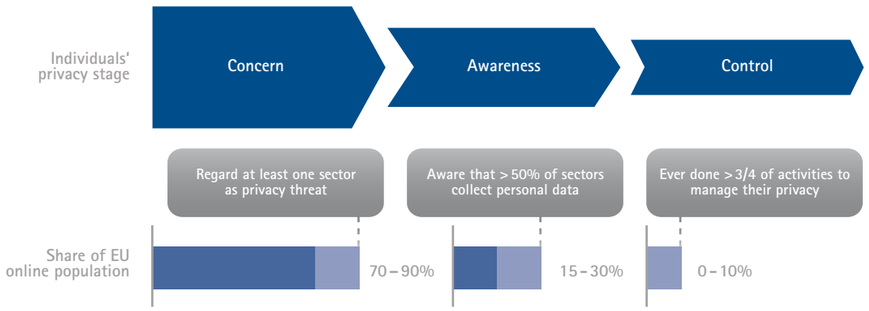
Many of these data breaches could have been avoided had organisations taken the proper precautions to safeguard information, such as using strong encryption to encode user account data, sufficiently restricting employee access to data and securing data backups. Their failure to take readily available steps only heightens consumer mistrust. It also causes brand and reputation damage when the breach occurs.

That last point is important, for the damages incurred when data is breached tend to be mutual: both consumers and organisations are harmed. Sony's PlayStation Network breach, for example, resulted in costs the company put at ¥14 billion by the end of its 2011 fiscal year – roughly €128 million.[11] Outside experts estimate total costs including brand damage at up to $4.6 billion.[12]

- **"What If" fears and worries:** These are the subjective concerns; the worries about "Big Brother" and other unscrupulous misuse. As employers take to social media sites to vet candidates and universities increasingly use them to screen applicants, individuals want to know that their information won't be used against them. They worry that new technologies, like face recognition, will give them less anonymity. They wonder whether companies and government agencies are creating detailed profiles on them, and how they might be using them. These, perhaps, are the hardest worries to allay, since they can't be solved simply by beefing up security.

New and emerging technologies can complicate the picture further, as many can be seen as both a privacy threat and a privacy enhancement. Biometrics can boost security by requiring a non-alterable, non-transferable identifying characteristic (a fingerprint, a retina scan, a facial pattern) for access. But it can also potentially be used to erode anonymity; for example, face recognition software that automatically identifies and tags social network users in photographs uploaded to the site.

Share of concern, awareness and control

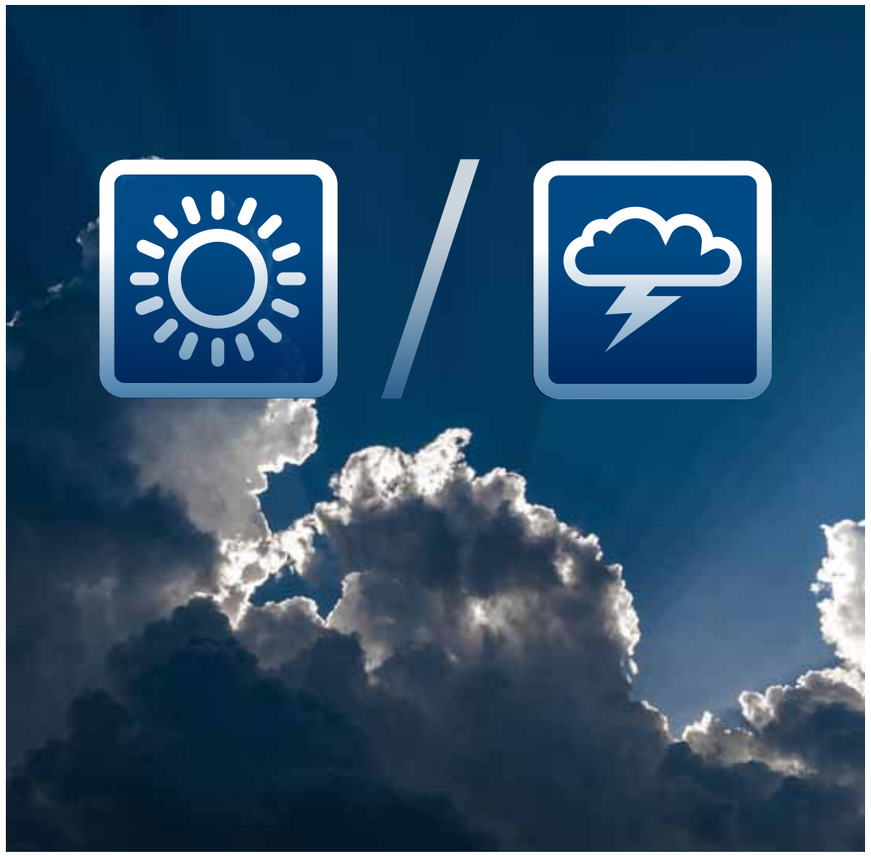


Source: BCG digital identity survey (n = 3,107, August 2012)

[11] Sony's script of revisions to reporting of fiscal year 2011 published on 23 May 2011

[12] Ponemon Institute 2011

A CONSUMER HAZARD OR DRIVER OF GROWTH, OR BOTH?



While most consumers are concerned about personal data applications, far fewer are aware of just how their information is being acquired and leveraged.

While most consumers are concerned about personal data applications, far fewer are aware of just how their information is being acquired and leveraged.

BCG's survey revealed that only 30% of respondents had a relatively comprehensive understanding of which sectors were collecting and using their data. Fewer still are able to exert some control over that collection and use. When survey participants were asked to note which of eight common privacy protection activities they had ever performed – actions like changing privacy settings in a social network, surfing the Web in "private mode" or disabling cookies in their browser – just 10% had ever done six or more of these things.

Consumers are largely in the dark about how, when and where their personal data is used. Transparency is often missing or insufficient – as evidenced by the 79% of survey respondents who said it should be improved.

When customers of the American retail chain Target Corporation signed up for the company's REDcard shopping card, they expected to gain benefits like special discounts. What they likely didn't expect – and what Target did not tell them – was that their purchase history was also being used to calculate a "pregnancy prediction score" for them (and a very accurate one, too, as expectant mothers tend to suddenly start buying certain products, like supplements and additive-free foods). For Target and other retailers, pregnant women are a valuable subset of buyers, since they tend to purchase more and with lower price sensitivity. But after Target started using those scores to develop lists of possibly pregnant customers and send them coupons for baby-related products, some of the recipients reacted badly – in one incident, recounted in The New York Times Magazine in 2012, an angry father confronted a Target manager after the chain guessed his teenage daughter's pregnancy before he did.[13]

For the retailer, the backlash was relatively minor. It simply tweaked the mailings so coupons for random products were included, too – making its targeted marketing appear not quite so targeted. But the incident demonstrates two crucial facts: Customers aren't likely to stay in the dark about data use forever (especially with the growth of social media), and companies run a real risk that when their customers do find out what is going on, they might do something about it.

Customers aren't likely to stay in the dark about data use forever, and companies run a real risk that when their customers do find out what is going on, they might do something about it.

This report will show that the risks companies face still exist and are significant. But it will also show that they can be reduced – to the benefit of consumers and organisations alike. This insight comes from the survey commissioned specifically for this report (and detailed in part 2), in which respondents from Germany, the Netherlands and Poland were presented with scenarios and questions that narrowed in on their attitudes – and their actual behaviour – regarding the sharing of data. What made this survey unique was that it didn't focus on the potential perils of sharing information so much as how the decision to share is made – the factors that influence it, and how consumers weigh them. This goes to the heart of what data-dependent organisations need to know as they try to strike a balance between value and privacy.

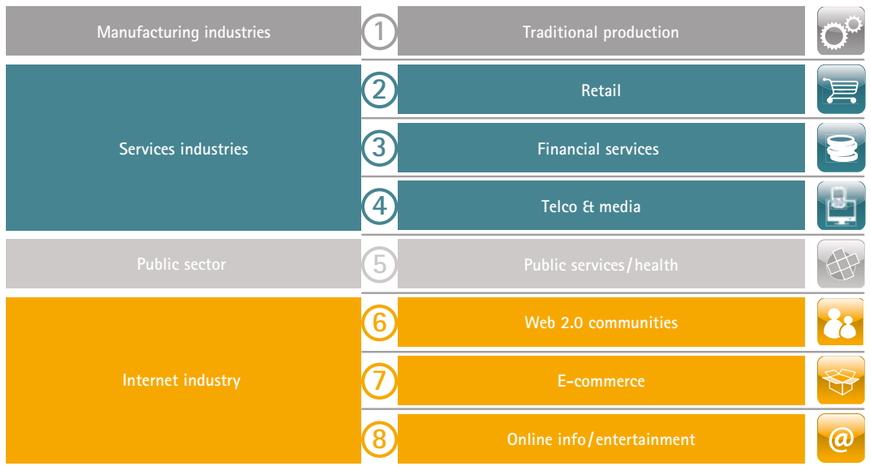
Balanced solutions protect privacy, generate value and create competitive advantage

Privacy and the way organisations treat consumers' data is becoming an increasingly important competitive factor. Anyone who doubts this need only look at the desktop and mobile Web browsing market. When Microsoft announced that its next version of Internet

[13] New York Times Magazine, 16 February 2012

A CONSUMER HAZARD OR A DRIVER OF GROWTH?

Analysed sectors



Explorer would enable a "do not track" feature by default – so Websites will know that a user does not tolerate cookies or any other tracking features – the move was clearly intended to lure customers away from competing browsers (like Firefox, Opera and Chrome) that are not expected to follow suit.

Another area where privacy and personal data management may likely be an important competitive dimension is the mobile operating system space. Worldwide, more than 850 million smartphones will run either Apple's iOS or Google's Android by the end of 2012.[14] Both platforms enable third-party apps to track highly sensitive personal data, like location information, once a user agrees to terms of use upon installation with just one tap. This model has already raised privacy concerns; consumers and policy makers alike are worried about data misuse by apps, particularly as the number of available apps continues to grow rapidly. Currently, neither Apple nor Google provide much in the way of user control. How they address the issue – whether they give users tools to manage their digital identities within the app ecosystem, or take no action – will have important implications in terms of both privacy and competitiveness.

Digital identity can change balance sheets – and change our future. But solutions need to put the customer front and centre. Only when there is trust that organisations are handling information responsibly and providing sufficient individual benefit, will data be shared in a sustainable way.

[14] Source: Gartner (July 2012); BCG analysis

This study aims to reshape the discussion by providing political and business leaders with a quantitative angle, empirical evidence on consumers' actual data-sharing decision making and a holistic perspective.

This study aims to reshape the discussion by providing political and business leaders with a quantitative angle, empirical evidence on consumers' actual data-sharing decision making and a holistic perspective.

In **part 2**, we present the results of a consumer research study that went beyond traditional survey questions on privacy concerns to look at actual behaviour. Drilling down on the factors that spur, and hinder, the sharing of personal data, it quantifies consumers' decision making, as well as their sensitivities.

Part 3 quantifies, for the first time, the current and potential economic value of digital identity for organisations and consumers. As the opportunities and challenges vary – often greatly –by industry and area, it takes a sector-by-sector approach, laying out the economic value, most important current applications and cutting-edge case studies for each. The result is a comprehensive, detailed overview of the value generation potential for the European economy as a whole.

In **part 4**, the report outlines the six most important trends of digital identity, the "megatrends" that are relevant for every organisation, in both the public and the private sector, looking to identify opportunities for value generation.

Finally, **part 5** presents a new paradigm for responsibly unlocking the value of digital identity – in a sustainable, consumer-centred way – and offers guiding principles for key stakeholders.

part 2

A DEFINITION OF DIGITAL IDENTITY AND HOW CONSUMERS REALLY SEE IT

A DEFINITION OF DIGITAL IDENTITY AND HOW CONSUMERS REALLY SEE IT

A DEFINITION OF DIGITAL IDENTITY AND HOW CONSUMERS REALLY SEE IT

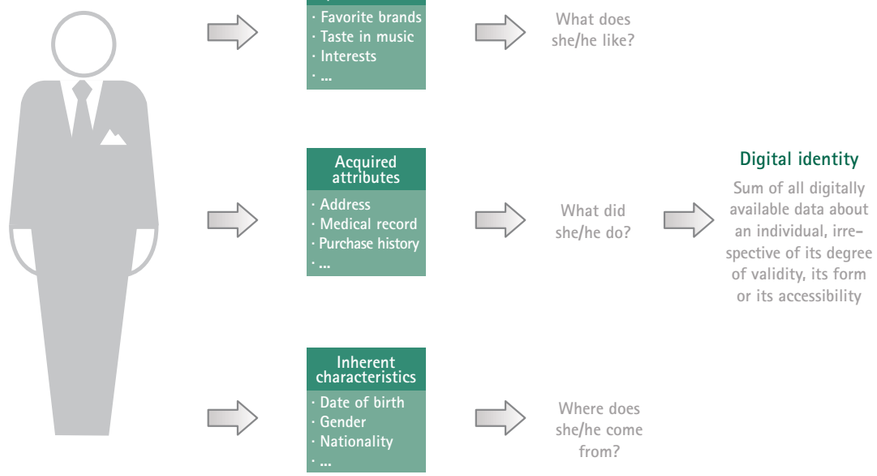
Digital identity: Putting the pieces of our lives together

By now, we are used to divulging little bits about ourselves as we navigate our physical and digital worlds: credit card information for a purchase; an e-mail address to receive discounts; a social security number on a medical form. By themselves, these pieces of personal data tell only part of our story; together, they form a richer, fuller picture.

That picture is becoming increasingly complete. The tremendous growth in the volume of personal data now shared or collected, along with advances in the ability to aggregate, process and gain insight from it, is not only making our digital identities more detailed, but also more accurate, more useful and ever more valuable. It is a phenomenon that is sparking innovation, anticipation and not just a little anxiety.

It is also a phenomenon that is often misunderstood, or not really understood at all. To that end, we define the key concepts involved in digital identity, share findings from a unique consumer research study and introduce an innovative framework for identifying the opportunities – and risks – presented by today's most important digital identity applications.

Digital identity definition



A definition of digital identity

Data about us – what we like, what we do, who we are – is scattered all across the digital landscape. It is distributed on different systems, on different storage devices, on social networks, on corporate servers, in government databases. No matter where it is, this information shares one important characteristic: It can be traced back to a specific person.

Digital identity is the sum of all digitally available data about an individual, irrespective of its degree of validity, its form or its accessibility. It can include any – and often all – of the following:

- **Inherent characteristics.** Where does an individual come from, and who is he or she? Date of birth, gender and nationality are examples of this type of information.
- **Acquired characteristics.** What is an individual's story; their history? Here, information such as address, medical record and purchase history are relevant.
- **Individual preferences.** What does an individual like? Data types here would include interests, hobbies and favourite bands and television shows.

The blurring lines of personal and anonymous data

The definition of personal data is fairly straightforward: information relating to an identified or identifiable individual. In the latter instance, the person would not be explicitly identified, but one or more aspects of the data record – such as a customer ID number or name and date of birth – could be used to trace it back to a specific individual.

Yet, as we will show, it is not always easy to determine what information can, and cannot, be traced back to someone. First, let's look at the different types of data from the least to the most traceable:

- **Anonymous data.** Data that is collected without any identifier and was never linked to an individual. An example of anonymous data would be a questionnaire returned by mail with no name or return address.
- **Anonymised data.** Previously identifiable information that has been de-identified: Anything that could link the information back to a specific individual – such as an ID code, a credit card number, even a serial number for a mobile phone – has been removed and a third party possessing the information would be unable to reconstruct it (if done properly, see below).
- **Pseudonymous data.** Data records that contain no clear ID, but an explicit identifier that can be used to link the data directly to a specific individual. Examples of such an identifier are a taxpayer ID or a customer account number. Pseudonymous data thus provides protection of personal data to the extent that the translation of the identifier into a clear ID is protected.
- **Clear personal data.** Information that is most easily traceable to an individual, as the data record contains a clear ID.

A DEFINITION OF DIGITAL IDENTITY

Organisations seeking to expand the use – and value – of personal information while mitigating privacy concerns often turn to a time-honoured solution: "anonymising" the data. The idea is simple: By deleting or obscuring the codes and identifiers that link back to a specific individual, any subsequent party using the data would have no way to know who it related to. Anonymised data is therefore key for many scientific and commercial applications of digital identity by third parties. After all, why should an individual mind if an organisation is sharing data that in no way identifies them?

But what is anonymous one day isn't always so anonymous the next. As the volume and variety of data grows – along with the ability to analyse it – links can sometimes be made even in the absence of explicit identifiers. With enough effort – and occasionally not much effort at all – the data can be traced back to a single individual. Sometimes this is done by comparing or piecing together different bits of data, a sort of high-tech deductive reasoning. Other times, a recently discovered technology makes it possible to unlock previously hidden or meaningless identifying details.

Consumers would likely be surprised – and concerned – by the speed and accuracy with which seemingly unidentifiable information can become identifiable. In one well-known example, two researchers at the University of Texas at Austin de-anonymised subscriber movie ratings that had been anonymised and published by the U.S. online video service Netflix (with random numbers replacing user names). By comparing the rankings and timestamps with ratings that had been posted on another site, the Internet Movie Database (IMDb), they were able to link some of the Netflix ratings with rankings that had been left, under a user's own name, on IMDb. This enabled them to identify the users behind those supposedly anonymous Netflix rankings.[1]

What this means is that organisations have to take special care and regularly revisit their processes when they want to use anonymised data – and determine whether the information is indeed truly untraceable. With each passing day, the odds are better that it's not.

Understanding how consumers view their digital identity

Organisations knowthat when they design a product or create a service, understanding consumer attitudes is a critical success factor. The same applies for digital identity applications. To leverage them successfully and realise the optimal benefits and value they can bring, one has to understand how consumers view their digital identity. What are their sensitivities? What factors do they weigh when making the decision whether or not to share personal data? And more to the point, *how* do they weigh those factors?

To help answer these questions, we commissioned a consumer research study – one very different from past research on the use of personal data. Traditionally, surveys on this topic have focused mainly on consumer attitudes. They ask participants about their opinions regarding how their personal information might be used. While these are important, words don't always equal action, and what is essential to know is consumers' actual behaviour. When presented with a choice to share – or not share – personal data, how do they *actually* make their decision?

To better understand that decision making, the study made use of conjoint methodology – a technique BCG frequently utilises in project work to identify how various dimensions of a product (such as the design, brand, cost and environmental impact of an automobile) influence purchasing decisions. In the same way, we used conjoint methodology to explore how different dimensions of data sharing (such as the type of data being collected, the sector doing the collecting and the method of collection) impact the decision to share personal information. This is the first time that such techniques were used in such a comprehensive way to analyse the privacy valuations of consumers.

The survey

A total of 3,107 Europeans were surveyed in the summer of 2012. The group was comprised of 1,026 individuals from the Netherlands, 1,041 from Germany and 1,040 from Poland; these regions were chosen because they offer a cross-section of Europe including countries with a reputation for high privacy valuation and a former Warsaw Pact country. Participants were selected as a representative sample according to the demographic factors of age, gender and region within their country.

The survey was split into two parts. The first followed a conventional path, with questions that explored attitudes and concerns regarding privacy (other questions obtained demographic data). The second part was designed around the conjoint techniques. Every participant was presented with 12 sets of "deals," each consisting of three scenarios in which payment was offered in exchange for data. The scenarios involved different types of data, to be put to different uses, collected in different ways, by organisations from different sectors. For each set, respondents picked the scenario, or exchange, they viewed most favourably.

Before carrying out the survey, we conducted numerous qualitative interviews to ensure that key names and descriptions were understood by respondents from different regions and backgrounds. Accordingly, we avoided technical terminology in the survey. For instance, instead of asking consumers whether they thought "opt-in" was necessary, we asked if they thought an organisation seeking to use their data ought to get their agreement beforehand. Using a standard test to gauge the accuracy of conjoint surveys – the root-likelihood analysis (RLH) – we found the resulting significance of this survey to be good.[2]

In the end, the study enabled us to quantify and visualise the willingness of individuals to share their personal data with organisations. The results – a key component of this report – will hopefully contribute valuable empirical evidence of how consumers view their digital identity.

[1] Narayanan, Shmatikov: "Robust De-anonymization of Large Sparse Datasets," 2008

[2] Root-likelihood (RLH) is 0.64. This implies that predictions based on the conjoint model are twice as good as random predictions.

A DEFINITION OF DIGITAL IDENTITY

Few consumers know how their data is used – fewer can control it

The survey revealed that while most consumers are concerned about their digital identity, fewer are specifically aware of how it is being used, and fewer still are able to manage it through privacy controls and other means. Our research also shed light on how these three dimensions – concern, awareness and control – impact the willingness to share data. Taking a close look at each, then, and understanding the role it plays in digital identity, is essential for developing applications that aren't just innovative, but also successful.

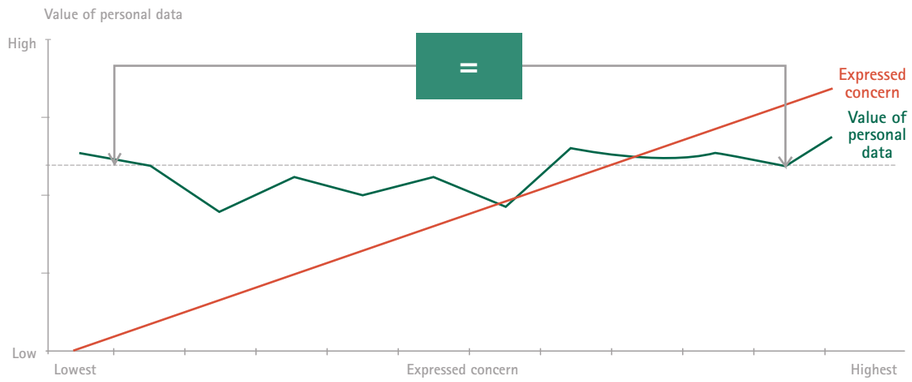
- **Concern.** To no surprise, given previous research and the public discourse, we found a high level of concern regarding the way organisations may be using personal data: 88% of respondents believed that at least one industry is a threat to their privacy. But the research also indicated that the level of concern consumers express is not a strong indicator of their actual behaviour when it comes to sharing data. When we looked at respondents at opposite ends of the anxiety spectrum – one group that expressed concern about the use of personal data by one or no industry sector, and another group that was concerned by all or nearly all of the sectors, we found that their actual privacy valuations (determined from the deal scenarios they chose, and reflecting their willingness to share) did not differ. In this respect, privacy is similar to climate change: Stated concerns do not necessarily translate into changed behaviour.

  The relationship between expressed concern and privacy valuation is shown below, in Exhibit *Expressed level of concern vs. valuation of personal data*. This "weak link" is not unprecedented: Previous research had found that an individual's stated concern about sharing private information was a poor indicator of whether or not they would join Facebook.[3] Our findings take this a step further – showing that the disconnect between individuals' concern and behaviour applies to the broader array of data-sharing scenarios.

- **Awareness.** The survey also revealed that consumers are largely unaware of what organisations are doing with their personal data. Only 30% of respondents had a relatively comprehensive understanding of which sectors[4] were collecting and using their data. This awareness gap, it turns out, poses a real risk to organisations, as the study found that consumers with higher awareness of data collection and use are less willing to share data. Specifically, those with higher-than-average awareness were, overall, 26% less willing to divulge personal information. A cynic might be tempted to think that ignorance is bliss – provided that ignorance can be maintained – or, to put it another way, that it is all right if an organisation keeps its use of personal data secret as long as it is very good at keeping it secret. But in this age of social media and viral communications, this is a less promising proposition than ever.

  Significantly, this correlation between awareness and willingness to share varies by sector, as shown in Exhibit *Impact of awareness on data sharing*. In retail, for example, the link is particularly strong: Consumers with high awareness are 53% less likely to share. For banks, however, high-awareness customers are just 13% less likely to share, and for public agencies, the figure is only 9%. It's worth noting that banks and public agencies have already a relatively high level of consumer awareness of collection and use practices. More than 80% of survey participants, for example, knew that banks were collecting personal data (ranking first among the sectors). Retail, on the other hand, rates the second lowest level of awareness, at just 32%. One possible interpretation: The more unexpected the use of personal data by an organisation is, the more pronounced is the effect of awareness on willingness to share.

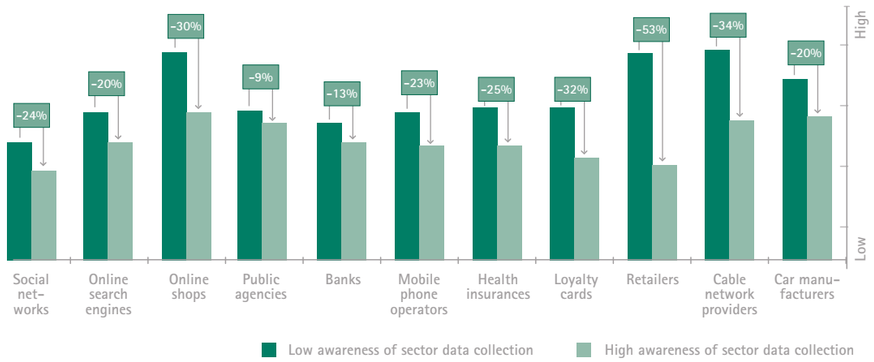
Expressed level of concern vs. valuation of personal data



Source: BCG digital identity survey (n = 3,107, August 2012)

Impact of awareness on data sharing

Impact of data collection awareness per sector on willingness to share per sector



Source: BCG digital identity survey (n = 3,107, August 2012)

[3] Acquisti, Gross: "Imagined Communities: Awareness, Information Sharing, Privacy on the Facebook," 2006

[4] While our research study focused on eight sectors, the survey included eleven types of organisations. We did this in order to capture the granular differences between different types of organisations within some sectors. For example, the public service and health sector is comprised of both public agencies and health insurers, who don't always use data, or impact an individual's views and behaviour, in the same way.

A DEFINITION OF DIGITAL IDENTITY

For a telling example of the low overall awareness of data collection and use practices, one need only look at Internet search engines. While 75% of respondents said they had shared personal information with organisations, only a quarter of these participants said they had shared such data with search engines. Yet at the same time, the overwhelming majority of respondents told us that they used search engines. As these sites almost always store search history – which often includes highly sensitive data – this was vivid evidence of the frequent disconnect between assumed and actual knowledge when it comes to what organisations do with personal information.

The takeaway for organisations seeking to create value through digital identity is clear: Low awareness can ultimately work against them – especially, if they conduct practices that consumers would not knowingly approve of.

- **Control.** Privacy controls also have an impact on a consumer's willingness to share, the research found – but in a positive way, if they are implemented well. The survey found that consumers who are able to manage and protect their privacy (via common actions such as changing privacy settings in a social network, disabling cookies in their browser, surfing the Web in "private" mode, or opting out of certain data uses) are up to 52% more willing to share information than those who aren't. Ease of use is critical, especially for low- and medium-sensitivity data. For sharing age and gender information, for example, individuals who had a relatively easy time managing their privacy were 37% more willing to share than those who had a relatively difficult time. (The correlation between ease of use and sharing does not hold for highly sensitive information, like medical and financial data.)

Impact of control on data sharing

Note: The privacy protection proficiency axis shows how many of the eight privacy-protecting activities respondents had ever applied, from lowest (none) to highest (all eight).
Source: BCG digital identity survey (n = 3,107, August 2012)

Exhibit *Impact of control on data sharing* shows how willingness to share varied with participants' proficiency in managing their privacy. Respondents were split into nine groups, corresponding to how many of the most common privacy protection activities they had ever performed. Participants with the lowest assumed ability to manage their privacy (those who had never performed any privacy protection activities) were also the least willing to share data. As user proficiency increased, willingness to share increased – though among the most proficient users, the correlation was not as strong (though they still had well above-average willingness to share).

It is significant, too, that few respondents were able to exert much control over the collection and use of their personal data. Just 10% had ever done six or more of the common privacy-protecting activities. And only around half had done more than three.

These findings lead to one crucial overarching conclusion: With easier-to-use privacy protection features, and privacy education, organisations might be able to significantly boost consumers' willingness to share data.

Why are consumers more willing to share when they have better controls? One idea is that individuals are more willing to take risks when they feel more in charge. Yet while this might be a contributing factor in their decision process, we would argue that choices and control simply help individuals adapt their sharing to their specific preferences. As we will show, preferences and sensitivities for personal data sharing vary widely among people – just as people themselves are different. We see these differing perspectives play out in real life all the time. For example, some frail and elderly individuals find it perfectly appropriate to have a video camera installed in their bathrooms, as a monitoring system to sound the alarm if they fall and get hurt. Very few young people, however, would want that same surveillance in their own bathroom.

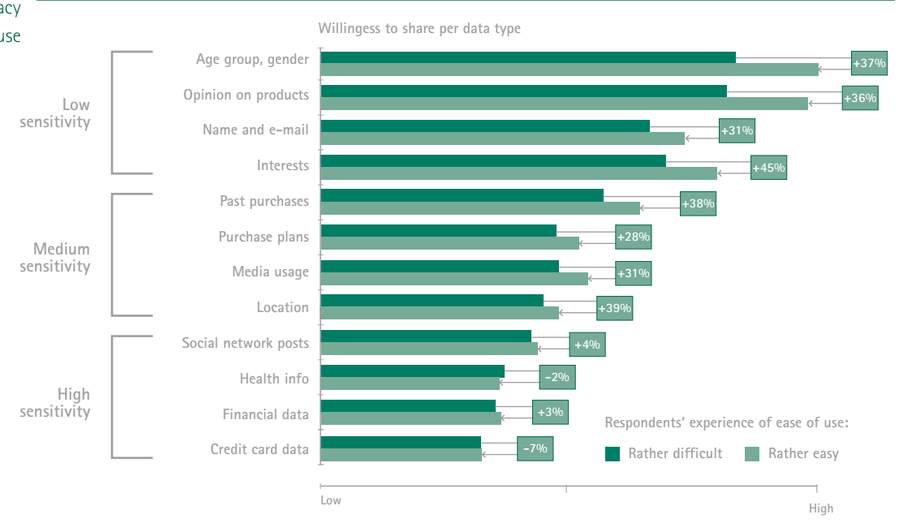
While accessible, intuitive privacy features have a positive impact on consumers' willingness to share personal data, the effect varies with the type of information at issue. As Exhibit *Impact of privacy protection ease of use* shows, the impact is great-est for data of low sensitivity (such as age, gender and interests) and medium sensitivity (past purchases and location, among other data types). But, as might be expected, the effect is neutral for highly sensitive types of data, like health and financial information. These are data types people would rather not share – no matter how easy it is to manage.

Many factors impact consumer decision making

The survey's conjoint methodology let us explore how different factors influence the decision to share, or not share, data. What we found was that consumers not only give different weight to different factors – the data type, for example, is more than twice as important as the collection method – but that even within a single dimension they make clear distinctions: For instance, consumers are on average nearly 30% more willing to share with cable operators and e-commerce companies than they are with Web 2.0 communities.

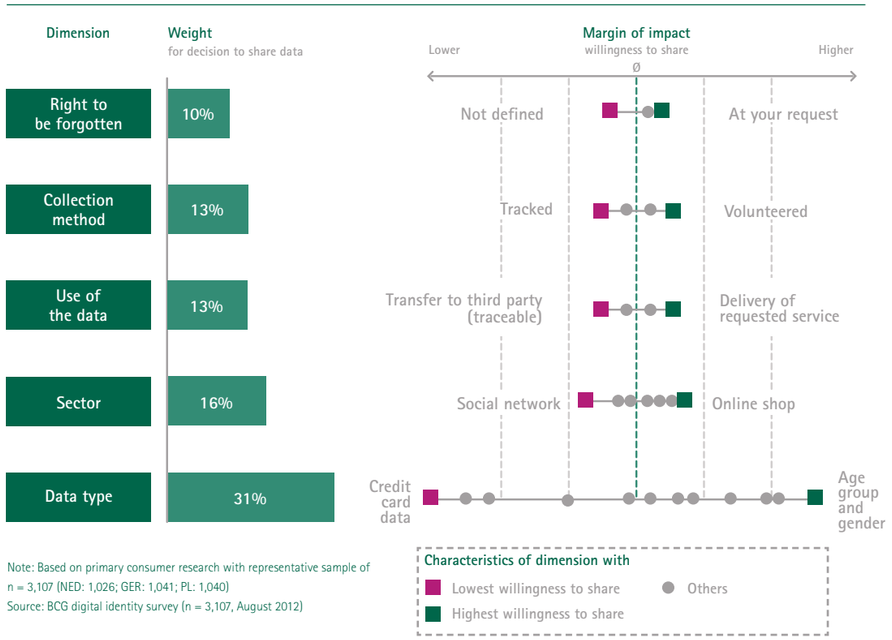
A DEFINITION OF DIGITAL IDENTITY

Impact of privacy protection ease of use



Source: BCG digital identity survey (n = 3,107, August 2012)

Dimensions of consumer decision to share personal data



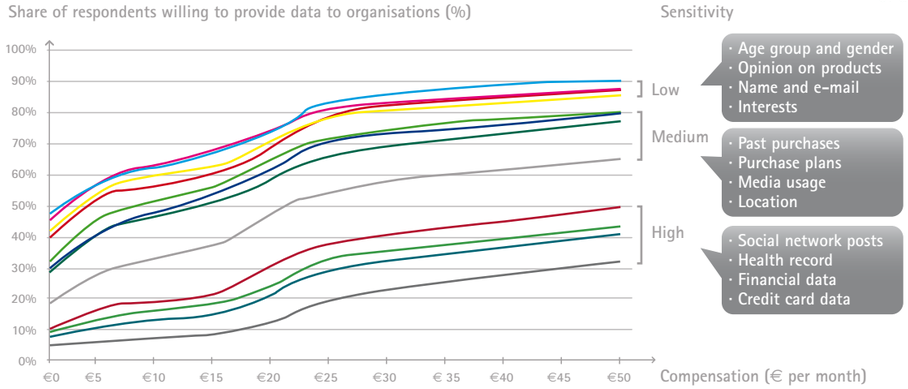
Note: Based on primary consumer research with representative sample of n = 3,107 (NED: 1,026; GER: 1,041; PL: 1,040)
Source: BCG digital identity survey (n = 3,107, August 2012)

In our research we explored how six major dimensions influence the consumer decisions to share personal data with organisations. In descending order of importance (to their decision making) they are:

- **Data type.** Not all data is considered equal when it comes to privacy. We found that consumers consider some types to be much more sensitive than others – and, accordingly, they are less willing to share it. There is more hesitancy to share credit card information, for example, than one's age group and gender. Financial data, health records, and social network posts are also considered very private; location data and past purchases less so; while interests, e-mail address and opinions on products are considered most readily shared with organisations.

Exhibit *Sensitivities of data types* shows how consumers differentiate between data types. While low-sensitivity information (like age and gender) was shared by more than 40% of survey respondents even without receiving a direct benefit, most participants were unwilling to part with highly sensitive data (such as a health record) even for large rewards. Notably, also social network posts belong to the category of highly sensitive personal data.

Sensitivities of data types



Source: BCG digital identity survey (n = 3,107, August 2012)

- **Compensation.** By increasing compensation[5], organisations can often – but not always – offset other factors that may be hindering the sharing of private information. The offset works particularly well for low- and medium-sensitivity data; less so for highly sensitive information, which, as seen above, is often withheld even when the compensation is high. While we tested cash compensation only in our experiment to achieve comparable results, for actual digital identity applications "compensation" can come in the form of many non-monetary benefits.

[5] It should be noted that the research method we applied provides very meaningful data on the relative differences, but the absolute monetary figures cannot be interpreted as the actual "value of the data." Rather they serve as indications of the value consumers place on their personal information.

A DEFINITION OF DIGITAL IDENTITY

- **Sector**. Consumer willingness to share personal data differs from sector to sector. The study found, for example, consumers are most willing to share personal data – about 13% more than the average of sectors – with e-commerce companies. On the other end of the spectrum, they demand far higher compensation from social networking sites than from any other sector.

- **Use.** How the data will be used – whether it will be used to provide the requested service, to enhance the delivery of another service or be transferred to a third party – also impacts the consumer's decision to share or not. The valuation is congruent in this instance with voiced opinions: Fully 70% of survey respondents disapproved of organisations allowing third parties to use data that could be traced back to consumers, while only 31% disapproved of organisations collecting data in order to deliver a product or service.

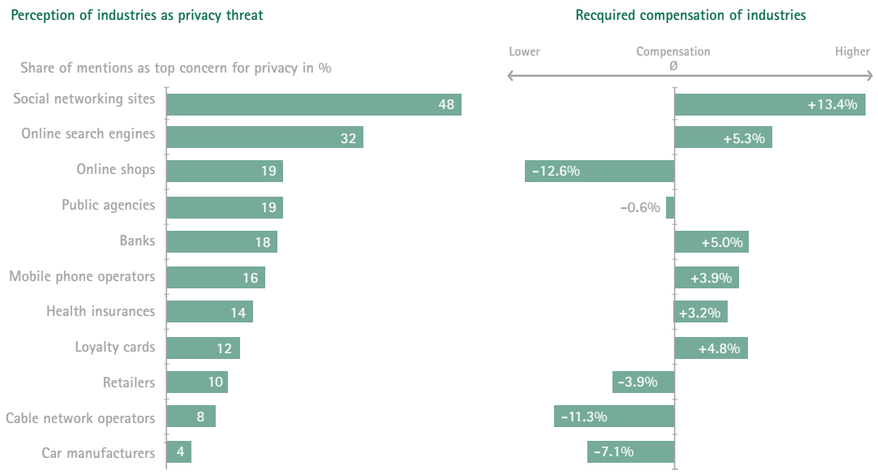
- **Collection method.** Consumers, the survey found, are more willing to share when the information is actively provided by them either voluntarily (e.g., date of birth provided in a form, despite it is not required) or because it is required for delivering a service (like address for shipping a package) than when it is acquired with them being passive via tracking (such as location data continuously transmitted by a consumer's smartphone) or data mining (information derived from analysing data sets).

- **The right to be forgotten.** Another factor consumers weigh is whether their personal information can be purged from organisations' repositories (whether this occurs manually on request or automatically after a specified time frame). The survey found that the impact of this right varies depending on the type of data at issue, but its presence has a positive impact on the decision to share for each one. The survey also found that the right to be forgotten is most significant for users with low overall willingness to share data.

As shown in Exhibit *Competitive position of industries*, the type of organisation seeking to collect and use personal data influences people's willingness to share. Social networking sites like Facebook have to provide consumers with 13% more benefit than other sectors, on average, need to in order to get the same data.

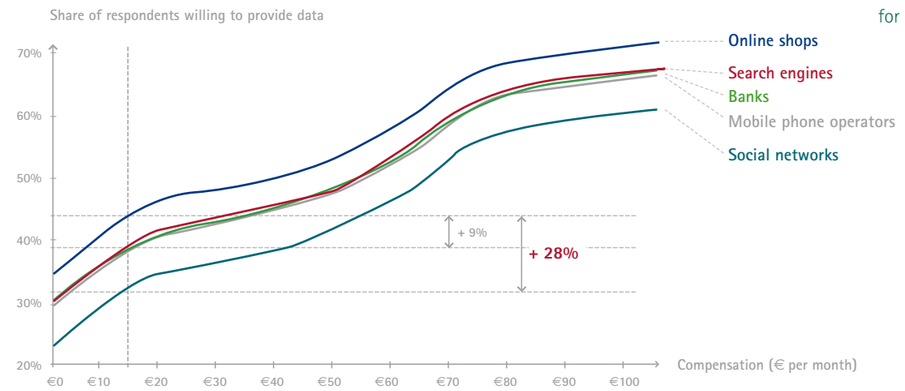
That consumers are more apt to share with some sectors than others can have significant ramifications for the development of some high-profile – and potentially high-value – digital identity applications. Case in point: digital wallets. Our research study revealed that e-commerce companies have a significant competitive advantage in acquiring the personal data needed for digital wallet applications; consumers were most willing to share the data with them (as depicted in the exhibit above). Ranking just below the e-commerce sector were search engines, banks, and mobile phone operators, all at a very similar level. Social networks, on the other hand, brought up the rear. One could argue that the e-commerce sector's high ranking reflects the experience consumers already have with it sharing data relevant for payment and offers based on users' purchase history. But whatever the reason, this is a strong indication that e-commerce companies are in a prime position

Competitive position of industries



Source: BCG digital identity survey (n = 3,107, August 2012)

Consumers' willingness to share data required for digital wallet per sector



Source: BCG digital identity survey (n = 3,107, August 2012)

A DEFINITION OF DIGITAL IDENTITY

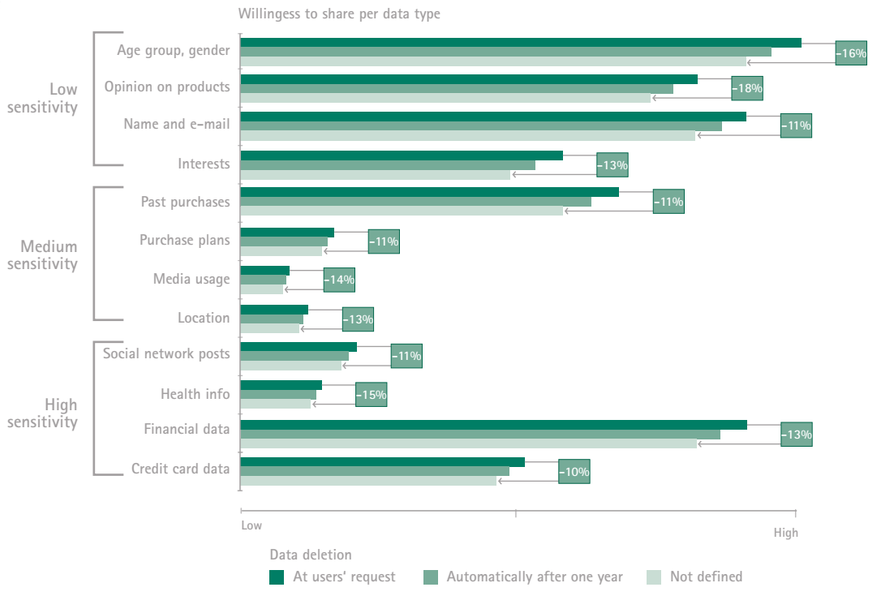
to get consumers' approval for the personal data usage required to provide digital wallet applications.

Consumer perspectives on the proposed EU privacy regulation

The study's research also shed light on how consumers view some of the privacy rights and controls in the EU's proposed General Data Protection Regulation:

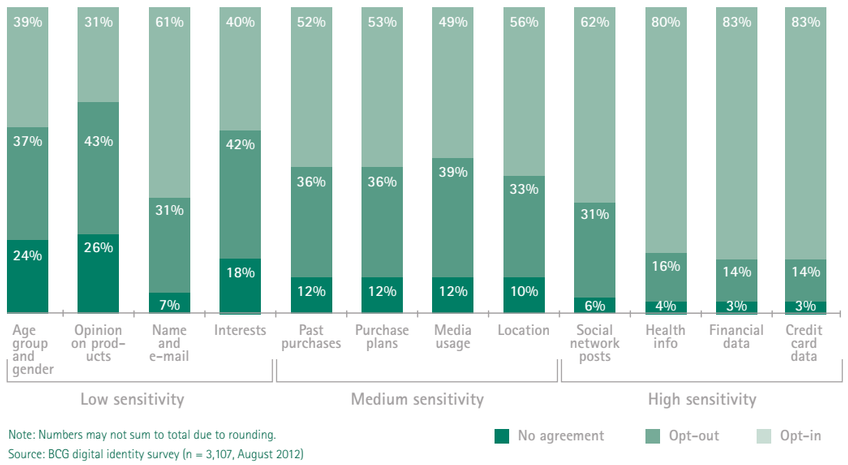
The right to be forgotten. As lined out above, this has a small but consistently positive impact on the willingness of individuals to share private data. When respondents were given the right to have their data deleted at their request – as opposed to deletion being outside their control – they were 10 to 18% more willing to share information (Exhibit *Impact of privacy protection ease of use* shows how this broke down per data type). This effect was most pronounced for people who had not shared private information with organisations before – or at least, didn't think they had.

Impact of the right to be forgotten per data type



Note: Based on primary consumer research with representative sample of n = 3,107 (NED: 1,026; GER: 1,041; PL: 1,040)
Source: BCG digital identity survey (n = 3,107, August 2012)

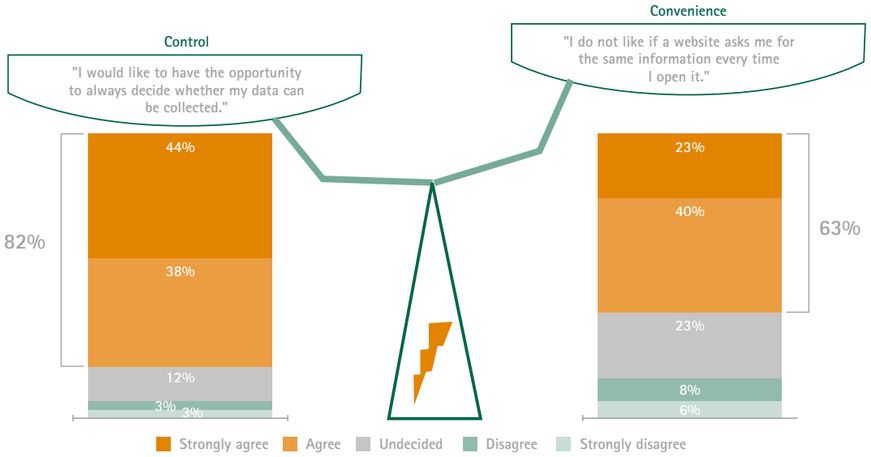
Consumers' view on consent



Note: Numbers may not sum to total due to rounding.
Source: BCG digital identity survey (n = 3,107, August 2012)

Consent. The form of consent consumers prefer strongly depends on the type of data at issue (see Exhibit *Consumers' view on consent*). For some kinds of less sensitive data, for example, up to 69% of respondents considered opt-out, or even assumed consent, appropriate. Yet when it

Dilemma of consumers' desire for control and convenience



Source: BCG digital identity survey (n = 3,107, August 2012)

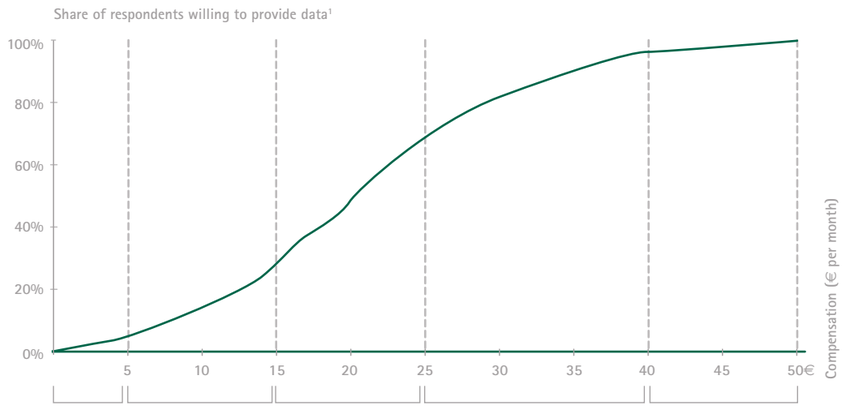
A DEFINITION OF DIGITAL IDENTITY

came to credit card data or financial information – among the most highly sensitive types of data – 83% of respondents said an opt-in mechanism was a must. With regard to consent, the survey also highlights a key dilemma digital identity poses: Consumers want more control of privacy, yet at the same time, want more convenience in the way they perform transactions and interact with organisations. As Exhibit *Dilemma of consumers' desire for control and convenience* illustrates, most respondents – 82% – expressed the wish to decide for themselves whether to allow data use in each instance. But a majority – 63% – also agreed with the statement, "I do not like if a website asks me for the same information every time I open it." Control and convenience are important aims. They are often conflicting aims, too. Balancing them will not be easy – but it will be critical.

Most consumers want to share their data – if the benefits and controls are right

Back in the 1990s, the renowned privacy researcher Alan Westin identified a specific segmentation of the population, three groups defined by their privacy views and behaviour.[6]

Segmentation along privacy value



[1] Scenario: Average for sectors and data types; data collection: "Actively, by providing data"; data use: "Allow other companies to use data anoymised"; the right to be forgotten: "Not defined"
Note: Segmentation for Germany
Source: BCG digital identity survey (n = 1,041 for Germany, August 2012)

- **The fundamentalists.** Comprising approximately 25% of the population, this segment is generally distrustful of organisations that ask for personal information. They are not willing to sell any private information, regardless of the incentives they are offered, and when given a choice, will always choose privacy controls over benefits.

- **The pragmatics.** The group comprises the majority of the population, about 65%. These individuals weigh the benefits of sharing their private information against the degree of intrusiveness. They believe that organisations, whether in the private or public sectors, should "earn" their trust and want the opportunity to decide for themselves whether to opt out of data uses. They are willing to share data if their privacy concerns are properly addressed.

- **The unconcerned.** Making up just 10% of the population, this segment is generally trustful of organisations that want to collect their personal information. They will readily give up privacy control to secure benefits and they are not in favour of enacting new privacy laws or regulations.

In the Internet era, 20 years is a long time, and our research shows that a significant shift in privacy valuation and behaviour has taken place since Westin formulated this segmentation. **Indeed, on the Internet today there are essentially no "fundamentalists" and no "unconcerned." Nearly the entire population are "pragmatics" – willing to share their data for the right benefit** (as shown in Exhibit *Segmentation along privacy value*). We found that only 5% of respondents had a very low privacy value, and less than 0.1% were giving all of their data away for free. At the same time, just 3% of respondents had a very high privacy value, and less than 0.1% would not share any data at all. While nearly all respondents fell into the "pragmatics" segment, we did find that privacy values differed by country. Dutch respondents had the highest (meaning they had the lowest average willingness to share), with Germans slightly behind and Polish respondents with the lowest average privacy value.

A framework for homing in on value and sensitivities

In part 3 of this report, we look at the key applications of personal data for each sector, as well as the less developed "cutting-edge" applications whose ultimate impact is hard to predict – but could be dramatic.

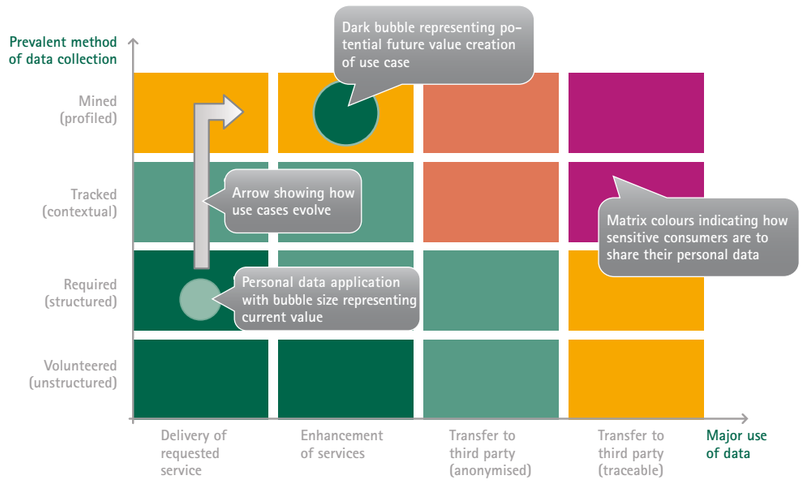
While the applications vary, a common framework can be used to evaluate every use case. This framework focuses on the two key dimensions in how digital identity is leveraged: the method of data collection and the manner in which it is used. Consumers consider these same two dimensions when viewing the trade-off between the value and cost of sharing information. Indeed, their willingness to share declines as the methods for collection and use move toward the outer boundaries; for example, when organisations acquire data via tracking or data mining, and when they sell it to third parties. Thus, consumer sensitivities can also be plotted on the same framework, and at a quick glance we can see both the opportunity and the risk any single digital identity application presents (as shown in Exhibit *Digital identity framework*).

Another lens through which to look at applications is the traceability and completeness of the personal data that is used. Individuals typically

[6] Alan F. Westin, 1991; Kumaraguru: "Privacy indexes: a survey of Westin's studies," 2005

A DEFINITION OF DIGITAL IDENTITY

Digital identity framework



prefer that businesses use digital identities that are incomplete and not traceable – data that may provide insight on usage or purchasing patterns, for example, but can't be linked back to a particular person. Organisations, on the other hand, generally prefer to use complete and traceable digital identities. Between these two poles, however, is space for compromise: solutions that balance privacy with value generation. For example, if control schemes guaranteed that digital identities remained untraceable, more complete identities could be used. Likewise, if data collection was limited to less complete information, more traceable digital identities could be employed. Just as organisations need to understand the impact of their collection and use methods, they must carefully assess the levels of traceability and completeness to be used in their applications and business models.

We hope that those frameworks, combined with the insight derived from the survey, will help organisations from all sectors to home in on applications that don't just offer value potential, but the balance necessary to realise it.

part 3

THE VALUE OF DIGITAL IDENTITY – FOR ORGANISATIONS AND CONSUMERS

THE VALUE OF DIGITAL IDENTITY

THE VALUE OF DIGITAL IDENTITY – FOR ORGANISATIONS AND CONSUMERS

While retailers and online businesses may have been the first to appreciate – and seek out – the value potential in digital identity, they now have plenty of company. Even organisations from the most traditional and least data-intensive sectors have received the message: There is opportunity in digital identity – opportunity to improve customer service, marketing efficiency, new product development and, in a nutshell, growth.

All told, the quantifiable benefit of personal data applications can reach €1 trillion annually by 2020 – with private and public organisations reaping about a third of the total, and consumers the rest (the latter explained in part by the high value consumers place on free online services they receive in exchange for their data). This may well turn out to be a conservative estimate, since we based it on today's major use cases, which represent only a subset of the applications we will see ten years from now. Nor does it include second-order effects, for example, if personal data applications improve medical care and prolong lives, that means people spending more money.

Yet opportunities – and the strategies to realise them – will vary from sector to sector. Key applications, as well as the drivers that make personal data available, also vary among the sectors. So, too, do the less developed applications, the cutting-edge uses of digital identity whose prospects are harder to assess.

Accordingly, in analysing the uses and benefits of digital identity, this report looks at the eight major sectors separately. For each, it explores key applications and where they fit according to the framework introduced in part 2. It looks at the potential benefits for both organisations and consumers, outlines case studies and notes applications on the periphery.

Quantifying the potential value of digital identity applications

To estimate the potential value of digital identity applications, we performed a bottom-up calculation based on the key use cases per sector. First, we identified approximately 20 core applications of personal data (such as targeted marketing, citizen self-service and loyalty programmes). Then, taking the sectors one by one, we developed a sector-specific business case for each application, based on data from research houses and public sources (e.g., development of population, development of market sizes), as well as BCG's own project work experience (e.g., benchmarks for efficiency improvements). Finally, for each use case, we derived a "digital identity value share"[1] to reflect the particular importance of personal data to that application.

For the purposes of this calculation, we defined value as follows:

- **Consumers:** The value for individuals includes the consumer surplus of Internet services[2]; lower prices (or taxes) resulting from organisations passing back efficiency gains they derived from using personal data; and time savings achieved via self-service and other digital identity applications.
- **Businesses:** For private-sector companies, organisational value consists of additional revenues along with the cost savings that remain after any "hand-backs" to consumers.
- **Governments:** The value for governments and the public sector includes increased tax revenues and spending reductions (nearly all of the latter, however, are expected to be handed back to citizens in the form of tax reduction or other relief).

Our quantifications do not include second-order effects. As those effects and as-of-yet unknown applications come to fruition, they will add to the value generated by personal data applications.

1. Traditional production

State of the sector

- **While digital identity is only beginning to be embraced, it is expected to be a key growth driver in an otherwise stagnant sector.**
- **Social media and in-product sensors are driving data availability, which in turn will drive new revenue-enhancing uses of digital identity.**
- **Targeted marketing, currently the main use case, will continue to grow in sophistication and importance.**
- **Personalised products and better customer insight promise significant benefits to consumers – both quantifiable (time and money saved) and unquantifiable (increased satisfaction).**

Traditional production companies like automobile and consumer goods manufacturers are quite familiar with the concept of "just-in-time" production. For them, digital identity can be considered a "just-in-time" revenue enhancer.

In a sector where growth has stagnated overall, several factors combine to give digital identity significant potential to create value. First, there is the explosive growth of social media, which is facilitating new channels of interaction with customers and generating an enormous amount of unstructured data: customer feedback, usage data, reviews and opinions. This type of information, and the insight it can reveal, has traditionally been hard to come by in the sector. Second, companies are starting to incorporate sensors in their products – devices that collect and transmit "back home" data such as usage and location information.

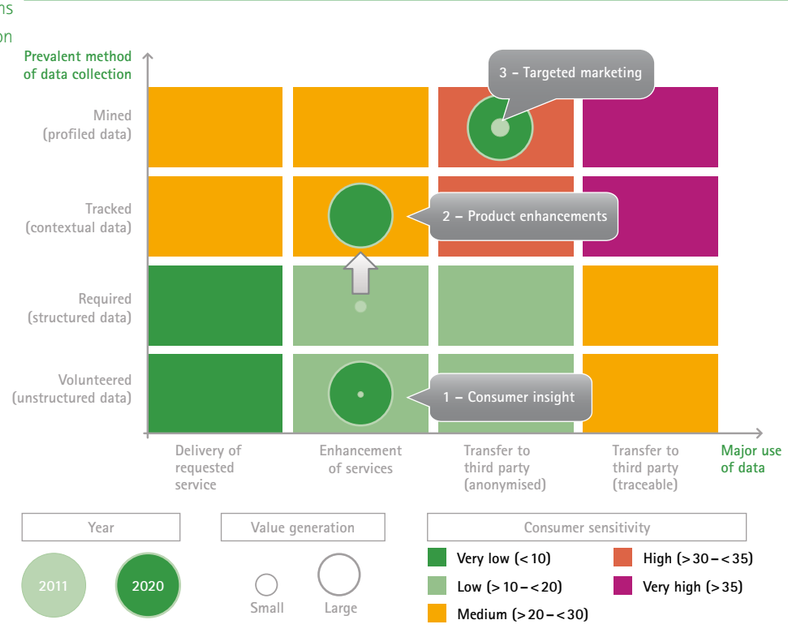
[1] See appendix: "Application of digital identity value shares in quantification model."

[2] The "consumer surplus" is the value Internet services (such as social networking sites) have for consumers beyond what they have to pay for those services (we include Internet access fees and device costs in their total payment); see BCG: "The Internet Economy in the G-20," March 2012.

THE VALUE OF DIGITAL IDENTITY

The dramatic increase in data availability will create an array of opportunities. Chief among them: enhanced and personalised products, new subscription-based services and targeted marketing campaigns. And make no mistake: The word is out. Big data expenditures – expected to reach $17 billion in 2015, with a 39% CAGR worldwide – are indicative of the sector's growing focus on converting data into value.[3]

Key personal data applications
Traditional production



Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

Key applications of digital identity

- **Consumer insight:** By collecting and analysing the increasing amount of consumer data that is available – from online comments on social media sites to real-time usage data transmitted by sensors – companies can develop products and delivery processes that are better suited to consumer needs. For example, Procter & Gamble's Vocalpoint provides an online forum to engage target customers in the development of new products (PUR water systems being one product shaped by this process).

- **Product enhancements:** By leveraging usage or location data transmitted by connected devices, companies can develop new subscription-based services or personalise existing products for additional revenue. A case in point: SNCF, one of the European railway leaders, developed a digital reservation and ticketing solution for mobile phones. It smartly leverages location data; for instance, a customer can purchase a ticket for the next train simply by passing the phone in front of a terminal on the platform. For SNCF, it is not just about transaction cost savings, but about giving consumers greater convenience and more choices.

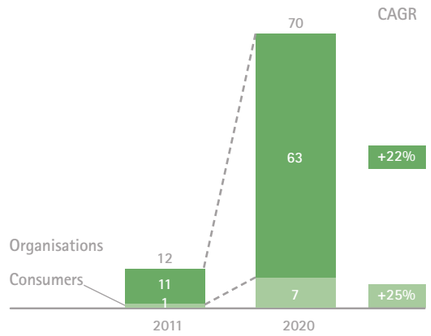
- **Targeted marketing:** As pioneered by the e-commerce sector, targeted advertising lets companies deliver more personalised ads to specific audiences defined by demographics or behaviour. The traditional production sector runs mainly branding campaigns and has been shifting these to the online space, increasingly leveraging targeting techniques to reduce waste. Certain forms of targeting can increase efficiency by an order of magnitude and, based on our project work in the digital marketing space, BCG considers an overall efficiency increase of 30% for branding campaigns to be realistic.

On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

- **Connected devices** that don't just monitor but learn. These devices analyse the daily habits or behaviour of users and adjust functionality and preferences accordingly. The new Nest thermostat, for example, learns when users tend to be out of the house, turning the heat down when they are at work and turning it up just before they come home.[4]

Digital identity value
Traditional production

EU-27 in 2011 and 2020, billion €



Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

- **Machine-to-machine (M2M) connections** that trigger preventive actions – and reduce product failures. Sensors in automobiles already track system performance. Taking this a step further, the data could be analysed for symptoms of potential trouble, enabling corrective action or early warnings to the driver.

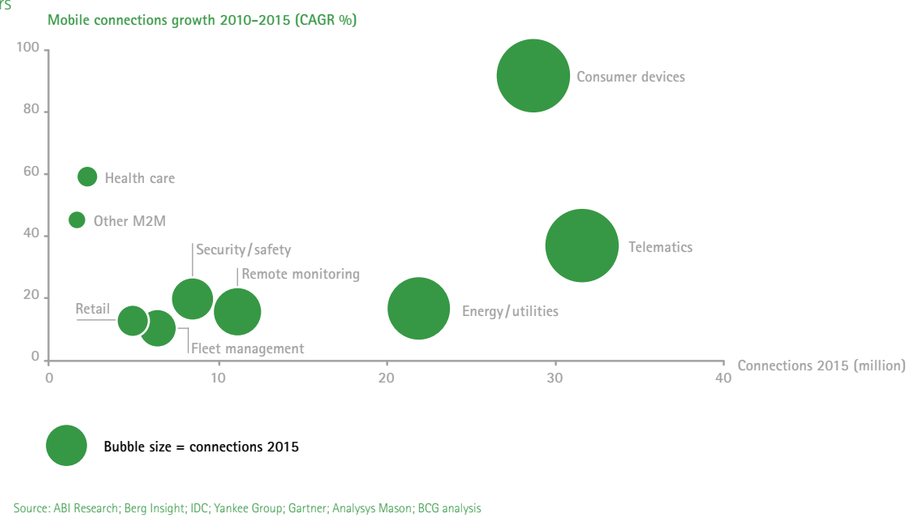
Computers and mobile phones aren't the only devices that connect to the Internet. Advances in communication technologies and miniaturisation – combined with cost reductions – have made it possible to give practically any product the ability to "phone home" or communicate with other machines. Indeed, by 2015, more than 75 million additional devices *other than* computers and phones will be directly linked to the Internet in Europe via mobile telephony networks. Potentially hundreds of millions more will be equipped with near-field communication

[3] Source: IDC (March 2012)

[4] www.nest.com

THE VALUE OF DIGITAL IDENTITY

Connected devices growth beyond mobile phones and computers



Source: ABI Research; Berg Insight; IDC; Yankee Group; Gartner; Analysys Mason; BCG analysis

chipsets like radio-frequency identification (RFID) or Bluetooth, which allow them to link with the Internet through other devices.

But it is *what* they will be communicating that will make things interesting. Onboard sensors – also more advanced and economical than ever – will measure all manner of information; first and foremost, usage data that can be linked to the device's owner. Collected, transmitted and analysed, this data can lead to insight that can be leveraged across the value chain.

Research and development efforts can be better focussed, thanks to usage data telling manufacturers what products and features customers like. Personalised products can be more easily, and creatively, developed. Trouble-shooting and preventive maintenance can be enhanced because devices can now literally sound the alarm when problems may be lurking.

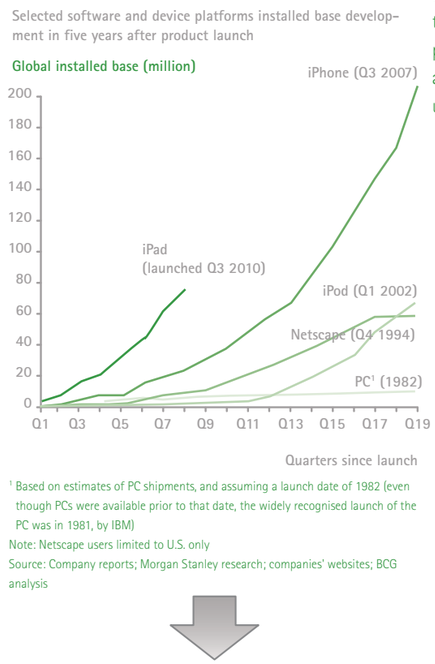
A second development sparking opportunities for personal data applications in traditional production is the increasing ubiquity of mobile devices. In Europe's largest markets, smartphone penetration is at 40% to 60% – and growing.[5] Meanwhile, Apple has sold more iPad tablets after two years than it sold iPods after five. The popularity of these connected devices, combined with their intuitive interfaces and ability to run third-party software, make them ideally suited to serve as "remote controls of life." Users will be managing all manner of products with just a few taps and in the process, establishing a connection between those gadgets and the Internet.

[5] Source: Gartner (July 2012)

The benefits for organisations and consumers

- Improved consumer insight helps companies improve delivery processes and better focus R&D efforts.
- Personalisation features make products more attractive to consumers, allowing companies to increase sales and/or maintain price points.
- Data-driven subscription services provide additional revenue streams and create a continuous relationship with customers.
- Targeted advertising maximises returns on a marketing investment, homing in on those consumers most likely to respond favourably.
- Personalised products bear tremendous untapped potential to save time and energy for consumers. Real-time traffic guidance and

Next-generation tablets and smartphones reach mass adoption at an unprecedented pace …



[1] Based on estimates of PC shipments, and assuming a launch date of 1982 (even though PCs were available prior to that date, the widely recognised launch of the PC was in 1981, by IBM)
Note: Netscape users limited to U.S. only
Source: Company reports; Morgan Stanley research; companies' websites; BCG analysis

… and will become the "remote control of life"

intelligent management of home energy consumption are still in the early stages of their respective life cycles.

RWE SmartHome – giving consumers control of their home energy consumption

In Germany, RWE launched SmartHome in 2010 to help its customers manage their energy use and costs. A family of devices – including thermostats, actuators and plug adapters – connect to lights, heating controls and appliances in the home. These devices are then linked to a central control unit through a wireless network. From a single interface on their PCs or smartphones, users can turn on, adjust or power down all of their lights, appliances, heating units and so on.

But the system goes even further: Users can create profiles to personalise – and optimise – their energy use, specifying, for example, when lights and heating should be turned on and off, or noting preferences like their preferred room temperature or how bright they like the lights in the living room. As convenience and comfort are enhanced, so, too, are savings. RWE expects that SmartHome can help to cut household energy costs by an average of 20%.[6] As energy use is reduced, pollution, carbon emissions and the drain on natural resources are decreased as well.

[6] Source: RWE

2. Retail

- **Retailers are already making extensive use of digital identity, aided by the availability of rich data sets derived from loyalty programmes and their ability to track transactions.**

- **The uses of personal data are relatively advanced – rivalling, and in some cases surpassing, the Internet sector. Partnering and sharing data with external parties, such as consumer goods producers and other retailers, is not uncommon.**

- **Current applications leverage digital identity to target personalised offers, improve internal processes and stock levels and gain customer insight.**

- **The mobile communications area presents a major opportunity. Real-time location data will allow retailers to more effectively deliver targeted, timely offers, and mobile applications will enable smaller retailers to launch loyalty programmes (solving the "no room in the wallet" problem).**

State of the sector

Continuous pressure on profit margins has given the retail industry plenty of incentive to leverage digital identity – and it has not let the opportunity pass. The sector is already making extensive use of personal information; by some measures more so, even, than the Internet sector. By tracking transactions and leveraging loyalty programmes, retailers have been able to gain insight on customer preferences and target their offers accordingly. They have also been able to reduce waste by optimising demand projections and stock levels. Further, the sector has actively embraced the larger data ecosystem, partnering with consumer goods producers as well as fellow retailers to share data and generate value from the added insight.

Looking forward, smartphones are revitalising loyalty programmes and targeted advertising, extending both their reach and their breadth. New mobile loyalty apps not only enable smaller retailers to set up programmes, but let companies push offers more directly to users. Real-time location data lets them deliver personalised offers at just the right moment, such as when a customer is near, or actually in, the store.

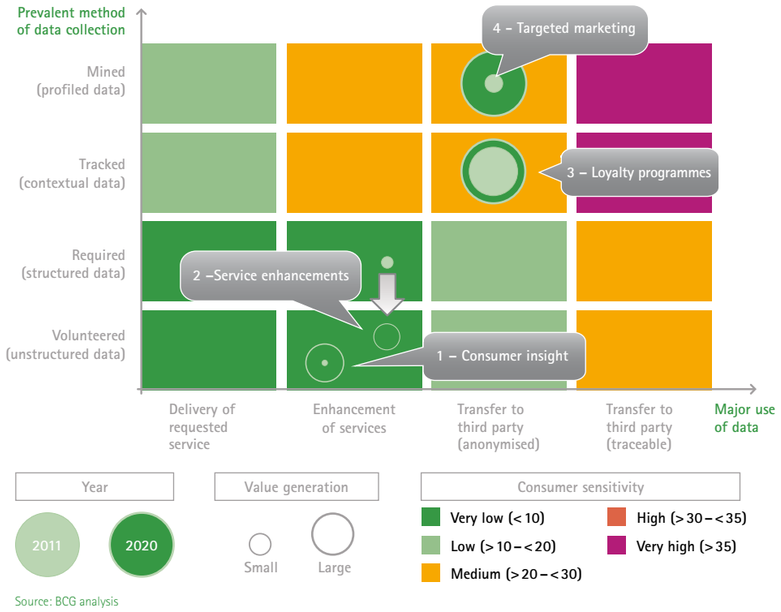
With retailers already leveraging digital identity for customer insight, targeted marketing, internal efficiency and partnerships with third parties, the potential for additional value growth appears considerably smaller than in other sectors. But this is an industry that has been on the forefront of putting data to work, and its embrace of cutting-edge applications, combined especially with the burgeoning growth of mobile devices, may lead to some unforeseen growth.

Key applications of digital identity

- **Consumer insight:** By analysing feedback and data in the social Web, retailers can improve their demand planning, product offering and process design. Fashion retailers are particularly proactive in this regard, as intimate customer knowledge can decide a season's success. Abercrombie & Fitch, for example, has more than 7 million Facebook fans, while H&M and Zara each

THE VALUE OF DIGITAL IDENTITY

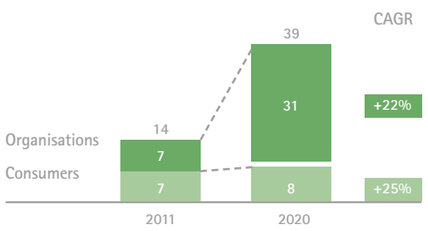
Key personal data applications
Retail



Source: BCG analysis

Digital identity value
Retail

EU-27 in 2011 and 2020, billion €



Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

have more than 12 million, and H&M has even 0.5 million people talking about its brand on Facebook.[7]

- **Service enhancements:** Companies can enhance the shopping experience through more active involvement of customers and integration of social Internet services. For instance, Woolworths Australia extended the grocery shopping experience to major commuter hubs with its virtual shopping wall and an accompanying smartphone app has been downloaded more than 1.5 million times.[8]

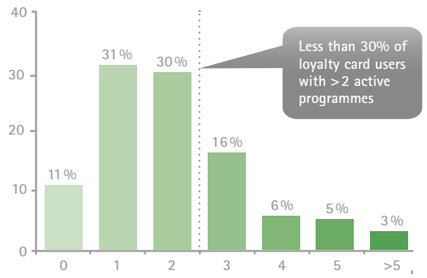
- **Loyalty programmes:** These programmes give retailers an effective way to collect and analyse a customer's purchase data and to communicate targeted offers. When executed well, they can increase revenues and customer retention. A particularly successful example can be found at Tesco. Its "Tesco Card" programme enables the retailer to thoroughly analyse customer data and create and send personalised vouchers. Tesco – whose loyalty programme members account for 80% of its sales – has a voucher redemption rate of about 15%, far above the industry standard of 1 to 2%.[9]

- **Targeted marketing:** Retailers have been at the forefront of leveraging digital data to deliver offers and advertisements to narrowly focussed groups of customers. Now they are extending this into the mobile space, sending offers directly to customers' smartphones and leveraging real-time location data to create and deliver offers that are both relevant and timely. Fast-food chains like McDonald's are leading the way.

On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

Current loyalty programmes' limitation

Number of monthly used loyalty programmes, % of loyalty members, global[1], 2011



[1] Average for U.S., United Kingdom, France, Germany, Brazil, China, Japan, India, Russia, and Canada | Source: Gartner; BCG analysis

Loyalty programmes have been a powerful tool for retailers, enabling them to incentivise repeat purchases (through rewards and discounts) while gaining insight about customers' purchases and preferences. However, traditional loyalty programmes have limitations. For one thing, there is only so much room in a consumer's wallet, apparently limiting the number of concurrent programmes consumers will use to two. Sign-up procedures can be cumbersome, and the programmes are very expensive to set up, putting them out of reach for most small and medium-size retailers. As a result, the retail sector has reached a saturation point for loyalty programmes.

Smartphones promise to shake things up, expanding both the reach and depth of these initiatives. Mobile loyalty apps and wireless integration with point-of-sale terminals mean that the device itself can be used in place of cards, adding convenience and creating a "bottomless wallet" where dozens of programmes can be as easily managed as two.

The mobile element also enables retailers to leverage new types of data and create innovative features and incentives for their customers. Mobile apps can transmit location data, enabling timely offers (for example, a discount delivered while the customer is in the store – or even the competitor's across the street). They could award points for scanning products that interest the customer or provide access to reviews. Consumers benefit from more relevant offers and information. Retailers benefit from greater customer insight – and an even deeper relationship than before. Nor would loyalty programmes remain the domain of the largest retailers; mobile

[7] Source: Socialbakers (October 2012)
[8] Source: Woolworths; press
[9] Source: Humby, Hunt and Phillips: "Scoring Points: How Tesco Continues to Win Customer Loyalty," 2008; press

THE VALUE OF DIGITAL IDENTITY

devices and apps open up the possibilities – and the payoff – to even the smallest shops.

- **Mobile loyalty apps.** Bringing loyalty programmes to smartphones offers several key advantages for retailers: It increases the reach of the programmes, enabling businesses to use real-time location data to send offers at opportune moments. It also enables smaller retailers – who otherwise could neither afford the setup costs of a conventional programme nor convince customers to carry one more card in an overstuffed wallet – to launch their own loyalty programmes.

- **Greater customer participation.** Mobile apps and social media enable customers to more actively communicate their likes and interests to retailers. Such insight can lead to highly effective personalised discounts. For example, the Wynsh app lets users photograph a product and ask for special offers. Since an individual discount has more value to a customer than a general offer, retailers can achieve the same result – a sale – with a lower discount.

- **Virtual shopping "walls."** Blurring the line between retail and e-commerce, this innovative application allows retailers to post visual representations of their products in public spaces such as subway stations. When customers see a product they want, they scan its barcode with their smartphone camera. After the purchase is authenticated, a home delivery is scheduled. Tesco Home Plus has built virtual shopping walls at public transport facilities across Korea. With a low capital expenditure, it was able to boost its online sales by 130%.[10]

The benefits for organisations and consumers

- Loyalty programmes – traditional and mobile – provide retailers with deep consumer insight, as all purchases can be tracked. They also boost customer retention and repeat purchase rates.

- Targeted marketing delivers relevant offers to those consumers most likely to respond, maximising the effectiveness of a marketing investment and reducing customer acquisition costs.

- Greater consumer insight lets companies reduce waste by better managing inventories, product offerings and internal processes.

- Real-time location data enables consumers to receive timely, relevant offers – which are particularly convenient when received near or in the store.

- Innovative mobile applications give consumers new and useful functionalities – such as communicating (via a photo or barcode scan transmitted by smartphone) what products they are shopping for, and receiving on-the-spot discounts.

Shopkick – an innovative mobile loyalty and retail marketing solution

Shopkick leverages an object nearly every shopper brings into a store: their mobile phone. The free app, which combines both loyalty and targeting elements, awards points – called "kicks" – to users each time they enter a participating store; additional points are earned for scanning products (using a smartphone camera). While there is a direct benefit to consumers – "kicks" can be redeemed for rewards or donated to charity – the payoff for retailers can be even greater. Shopkick drives foot traffic into stores, while the data it collects – including location and interests – drives sales. Retailers can offer highly relevant deals and discounts while the user is still in the store. In 2011, $110 million in retail revenue could be linked back to Shopkick.

With more than 3 million users and 7,000 participating stores – including major chains like Best Buy, Old Navy and Target – Shopkick demonstrates that well-crafted, non-intrusive mobile apps can be a boon to both retailers and shoppers.

[10] Source: Tesco; BCG analysis

Innovative approaches in retail

wynsh — Wynsh puts customers in driver's seat of marketing …

You decide where your discount should be offered

App identifies nearby participating stores

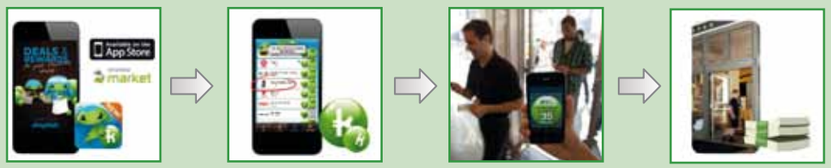
User photographs products of interest

Photos are sent to retailer

Retailer grants individual discount to user

* Discounts granted are variable and are set by the brand in question.

Shopkick — … and Shopkick increases loyalty reach



User installs app on smartphone

App identifies nearby participating shops and restaurants

Device in stores automatically registers walk-in and user gets "kicks" points

User can redeem collected "kicks" for discounts and free services

Source: Wynsh; Shopkick

THE VALUE OF DIGITAL IDENTITY

3. Financial services

- **Banks and insurance companies possess a wealth of data due to their everyday business.**
- **The current major use case is process automation – especially customer self-service – but the sector can significantly increase digital identity value by moving beyond these core applications.**
- **Increased use of mobile devices will not only make more data available in real time (such as location and transaction information), but will allow sector companies to develop personalised services and enhance their targeted marketing efforts.**
- **Mobile wallet applications are potentially lucrative – but only if the purchasing data collected can be used or monetised by way of targeted advertising.**

State of the sector

The financial sector possesses an enormous cache of personal data as a result of its everyday business. That volume is only going to grow with increased use of electronic payment methods. Meanwhile, the burgeoning use of mobile devices will provide new data types – in particular, location information – and make them available in real time. This wealth of data will mean a wealth of possibilities.

So far, the sector is just scratching the surface of what it can do with digital identity. The major use case is process automation; primarily, self-service transactions through the Web and, increasingly, mobile. These efforts are paying off handsomely: Online and mobile transaction costs run about 5% of their in-branch counterparts.[11]

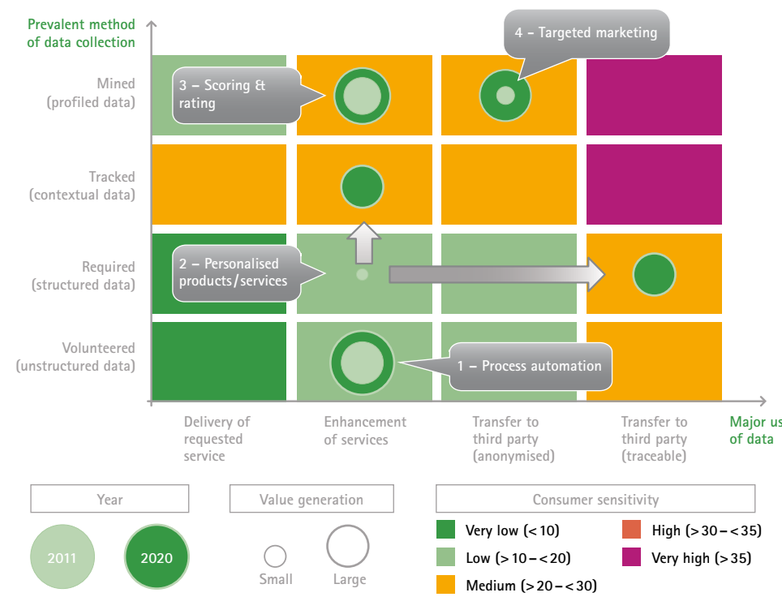
There is much more potential to tap. The sector can boost the value it creates with digital identity fivefold by moving beyond core applications. Some of these we are already starting to see, in more sophisticated uses of data to personalise products, more accurately score and rate potential customers and target advertising.

The mobile space offers even more possibilities, including digital wallets and mobile payment, as well as the ability to target advertising and even product offerings based on real-time location data.

Key applications of digital identity

- **Process automation:** Customer self-service – through the Web or mobile applications – provides an automated, anywhere-anytime alternative to more expensive and more time-consuming phone or in-branch transactions. But automation can mean much more than simply paying bills or checking an account balance. For example, AXA Insurance has developed a smartphone app that lets customers file claims right at the scene of an automobile accident. They can use their mobile device's GPS capability to find the closest approved repair shop, and even tap a button to place a call for a tow.

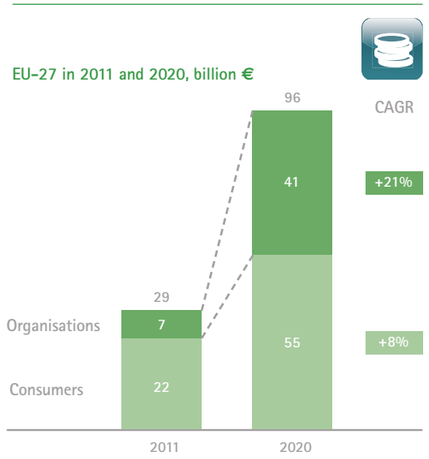
Key personal data applications
Financial services



Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

- **Personalised products/services:** New data types (such as location and usage information) available via mobile devices and sensors allow for an array of innovative products. GM's OnStar system, for example, is a subscription-based service in which an in-vehicle device captures diagnostic and usage data (such as mileage) and provides navigation and roadside assistance. Through a partnership with GMAC Insurance (and with driver permission), usage data is sent to the insurer, which can result in a low-mileage discount.
- **Scoring and rating:** By accessing and interpreting data from additional available sources, such as the social Web, companies can improve

Digital identity value
Financial services



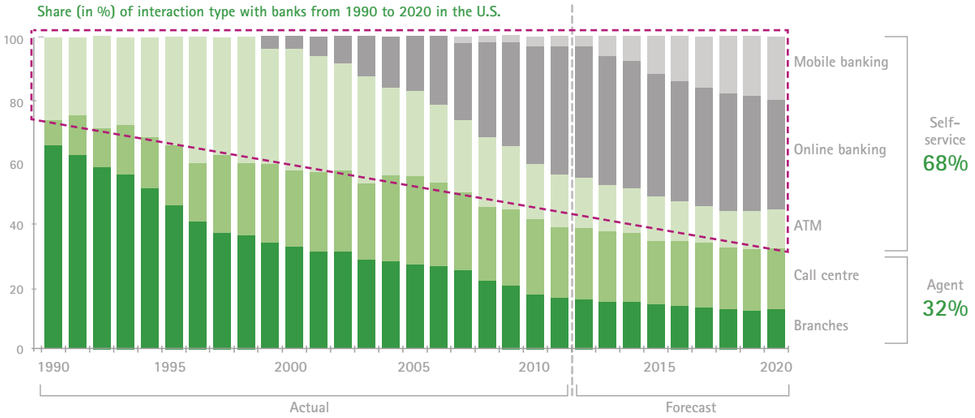
Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

[11] BCG analysis

THE VALUE OF DIGITAL IDENTITY

their scorings of customers, thereby improving risk management and fraud prevention. Case in point: Aviva ran a trial with 60,000 individuals in the US in 2010, showing that online data detailing food purchases and social activities could be as effective in identifying potential health risks as blood and urine tests. Although this practice is highly controversial, with critical questions regarding individual consent yet to be answered, this example illustrates how much insight about a person can be derived from such data.

Development of self-service in banking



Source: NRC; Deutsche Bank research; Forrester; BCG analysis

- **Targeted marketing:** Companies are using the growing amount, and detail, of personal data to more efficiently target their marketing activities – homing in on specific audiences instead of a more general placement.

Banking transactions tend to be high-volume, standardised processes – a balance inquiry, a transfer between accounts, a credit card payment. That makes them particularly well suited for customer self-service. Automated teller machines were an early example of "bankerless" banking and demonstrated that by taking humans out of the equation, banks could save transaction costs while improving customer convenience by increasing availability of the service.

With the rise of online and mobile banking, customers are able to not only serve themselves, but to do so from any place, at any time. Little wonder, then, that self-service now accounts for nearly 50% of all bank transactions, more than double the figure from the early 1990s. And the upward trajectory will continue, assisted by biometric technologies that will enhance authentication and convenience (no pass codes to remember). By 2020, ATM-based, mobile and online self-service will account for nearly 70% of all bank transactions, and walking into a branch will be an increasingly infrequent event. Good news for those who'd rather spend their lunch hours elsewhere.

On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

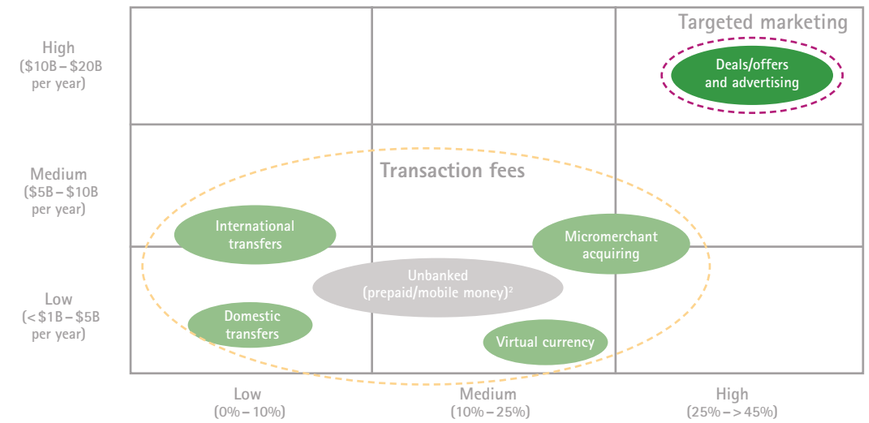
Intensified use of location data to innovate services. The location data provided by mobile devices can help companies match the right customer with the right offer – at the right time. For example, insurer Tokio Marine, in cooperation with mobile network operator NTT DOCOMO, offers specialised one-time insurance policies – via mobile devices – based on a user's location and inferred activity (e.g., golf insurance for someone currently approaching a golf course).

Basing insurance premiums on actual, rather than predicted, behaviour. As telematics-capable devices emerge – recording everything from how far an individual walks each day to how fast they drive their car – they will enable insurers to base premiums on actual activities and behaviour instead of statistics and predictions. This will give consumers additional choices, like paying car insurance only for the miles actually driven.

Digital wallets. While not presently a mainstream payment option, an increasing number of mobile handsets are coming equipped with near field communication (NFC) technology, which will allow consumers to complete a transaction simply by holding their phone to a point-of-sale unit. In itself, these payment transactions will not lead to significant revenue gains. But the data that is collected can give valuable insight

Digital wallet / m-payment revenue pools

Digital wallet revenue pools in billion USD p.a. and competitive intensity[1], 2015



[1] Percentage of business pursuing business opportunity (based on 100 companies observed)
[2] Relevant only in emerging markets with undeveloped banking system
Source: BCG: "How Banks Can Take the Lead in Mobile Payments," June 2012

THE VALUE OF DIGITAL IDENTITY

about a consumer's interests and preferences – insight that can make financial companies an important player in the targeted advertising space and open up new revenue pools.

For the financial services sector, digital wallets, or mobile payments, will bring transaction fees from three major sources in developed markets:

- Domestic and international transfers diverted from traditional payment channels (digital wallets are expected to capture just a small share of the overall transaction volume).
- Payments in the virtual world, where consumers look for alternatives to credit cards.
- Payments to small merchants who lack credit card terminals, and to larger merchants instead of cash payments.

Yet transaction fees are just a part of the potential revenue digital wallets can bring financial services companies. Advertising that is targeted based on mobile payment data is, in our estimate, up to 10 times more valuable to marketers than advertising targeted according to context or behaviour. This makes the data recorded by digital wallet applications highly valuable as well.

Nor are the finance companies the only ones to benefit. Brick-and-mortar merchants will be able to measure how online advertisements impact offline purchases, so they can gauge – and improve – the efficiency of their campaigns accordingly. That's a capability e-commerce companies have long enjoyed, but traditional retailers had previously lacked.

Before the full potential of the digital wallet can be realised, however, there has to be widespread acceptance of it by merchants. The increasing availability of near-field communication in smartphones, as well as point-of-sale technologies that use it, is a hopeful sign that we may not need to wait for long.

The benefits for organisations and consumers

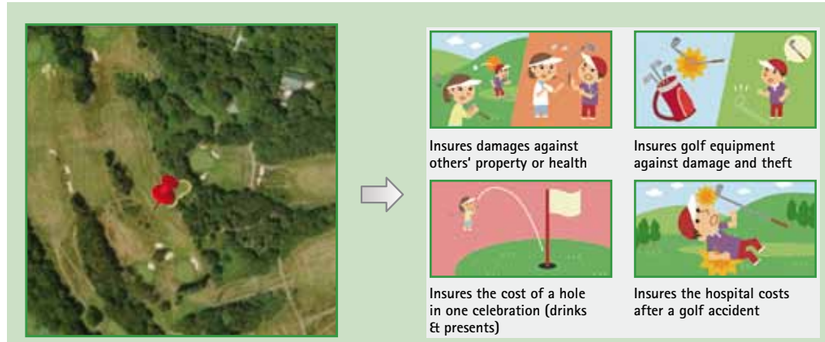
- Process automation enables a company's IT systems to do the work of more expensive manual processes.
- Personalised products and services enhance the sales potential of existing revenue streams and open up all-new ones.
- The insight that can be gleaned from purchasing data can be monetised via sale to, or partnerships with, advertisers and other organisations.
- Targeted marketing allows companies to more cost-efficiently reach those consumers most likely to respond, maximising the impact of a marketing investment.
- Consumers save time and gain convenience through anywhere-anytime self-service transactions.
- More accurate scorings and ratings lead to fairer pricing for insurance and other services.

Tokio Marine Nichido and GMAC: Innovative one-time and "pay-as-you-drive" insurance policies

Smartphones and sensors make it possible to capture real-time location and usage data – and already, that is transforming the way

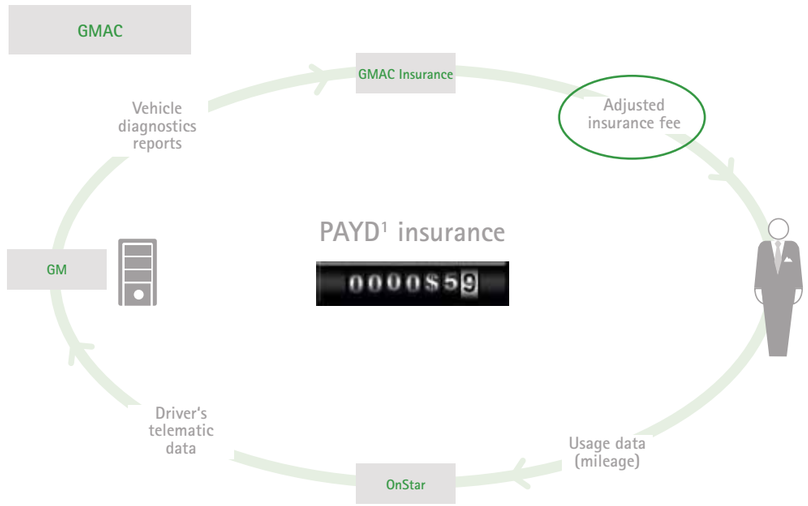
Location-based one-time insurances

Tokio Marine Nichido



Source: Tokio Marine; NTT Docomo

Pay-as-you-drive insurance



[1] Pay-as-you-drive
Source: GM; GMAC; OnStar; BCG analysis

THE VALUE OF DIGITAL IDENTITY

some financial products are sold. Case in point: insurance.

In Japan, telecommunications giant NTT DOCOMO has teamed up with the insurer Tokio Marine Nichido to offer innovative "one-time" policies based on a mobile phone user's location. Through the GPS capabilities on a smartphone, a user's location data is acquired, and from it, behaviour can be inferred. For example, someone located in an airport is likely taking a trip; someone on a golf course may be playing a round or two. The service then sends a message to the phone, offering a relevant policy. NTT DOCOMO gains a new revenue stream from location data it already collects, and Tokio Marine Nichido is able to offer just the right policy at just the right moment. Services like these also open the door to new, specialised insurances for all manner of activities and situations.

Meanwhile, in the United States, fairer automobile insurance premiums – based on actual, rather than predicted, driving behaviour – are now possible, thanks to in-car devices that collect and transmit usage data like mileage. OnStar, from General Motors, is a subscription-based service that has tradi-tionally used such data to provide navigation and diagnostics. Now it is being used to get low-mileage drivers lower insurance premiums. For a fee, GM sends OnStar data to GMAC Insurance, which then uses it to adjust insurance premiums according to actual miles driven. The result: a win across the board. Consumers save on insurance, GM monetises data while incentivising more drivers to subscribe to OnStar and GMAC improves its insurance pricing – and gains a competitive advantage among a crowded field of rivals.

4. Telecommunications and media

- **Companies have access to a vast amount of personal information mainly relating to telephony usage or TV-viewing data, but so far make relatively little use of it.**
- **Digital identity is expected to be a huge growth driver in a sector where growth and competition is closely linked to the ability to innovate and enrich existing services.**
- **Currently, the chief application is process automation (in particular, customer self-service), which is helping to reduce the traditionally high level of operational expenditures in this sector's service-provisioning processes.**
- **Like the financial sector, telecommunications, cable and media companies can see a fivefold increase in digital identity value by moving beyond core applications.**
- **The trust that customers put in their network providers critically depends on their commitment not to track behaviour over their networks other than for purposes related to service delivery, unless customers give their consent.**

State of the sector

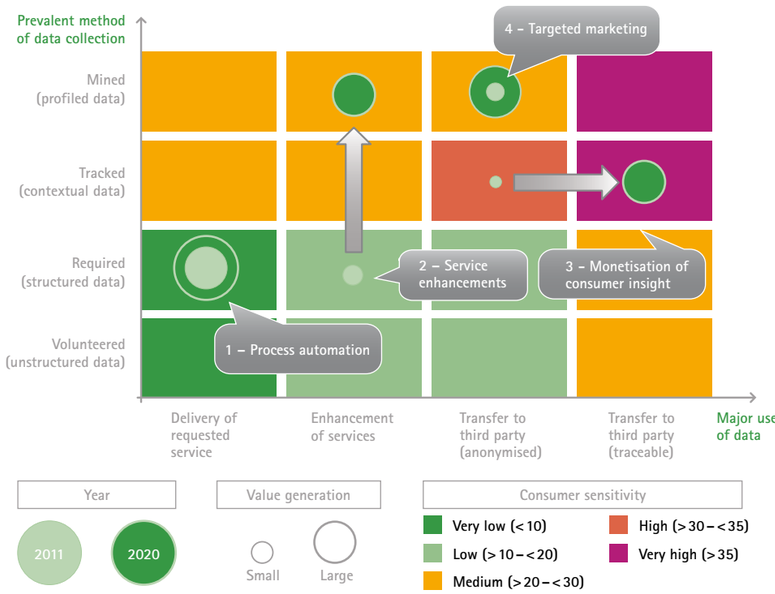
For telecommunications and media companies, digital identity holds the promise to cushion – considerably – the impact of an increasingly competitive marketplace. The relief won't come a moment too soon. Disruptive IP services – Skype, YouTube and Spotify, to name a few – threaten the revenues generated by their core services, putting companies under pressure to develop higher-value services while streamlining costs.

Sector companies have, in principle, access to riches of data. But there are serious caveats. Telecommunications and cable companies operate the fixed and mobile networks that data passes through – putting them in a prime position to capture usage and location data – but, under EU electronic privacy rules they cannot collect and use data, such as traffic data or location data, unless users have given their prior consent. Users can also withdraw prior given consent at any time.

Like financial institutions, this sector is only starting to explore the possibilities of data-driven value creation, and current applications fall far behind the Internet and retail sectors in their sophistication. Currently, the chief use case is process automation. This is no small thing, given that many companies still incur significant operational expenditures for their provisioning processes, and the shift to customer self-service and the resulting efficiency gains can be a large value driver. But by moving beyond core applications, telecommunications and media companies can increase digital identity value fivefold.

Developing and benefiting from those new applications may nevertheless require a careful approach, as subscribers need to be able to trust their network operators to guarantee the

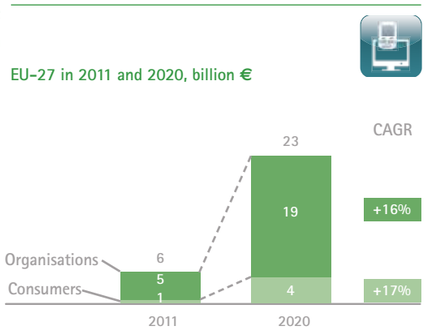
Key personal data applications
Telco & media



Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

THE VALUE OF DIGITAL IDENTITY

Digital identity value
Telco & media



Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

confidentiality of communications over their networks. But if they tread carefully and transparently with regard to intended data collection and usage processes, and consumers are given an informed choice to consent, network operators would be in a prime position to capture usage and location data (which it-self can be monetised). They could also facilitate partnerships to attract third-party applications to their digital platforms – relationships where another sector's expertise and this sector's data combine to create value for both.

Key applications of digital identity

- **Process automation:** Through the use of secure digital authentication, companies can enable customers to perform transactions in self-service or completely automate them, both online and with mobile devices. This can reduce manual effort and costs – sometimes considerably. But it often requires rethinking processes end-to-end; for instance if a product portfolio is too complex, people will have to go to shops so it can be explained by a sales clerk, no matter how well the online ordering process works.

- **Service enhancements:** By leveraging data provided by or inferred about users (such as location data captured by mobile devices on the network), companies can develop – on their own or in partnership with other sectors – personalised services that increase usage and revenue. Case in point: Netflix, the video streaming and rental service, claims that its personal recommendations algorithm is responsible for 75% of what subscribers watch.[12]

- **Monetisation of consumer insight:** The data that companies capture, or the insight derived from it, can be sold to third parties for use in their own services. For example, Telefónica has set up a business unit – Dynamic Insights – dedicated solely to seizing the opportunities presented by the company's data wealth. Its first commercial product, "Smart Steps," will leverage location data to help retailers better understand what drives foot traffic to their stores.[13]

- **Targeted marketing:** Leveraging personal data (including real-time location data provided by mobile devices on the network), companies can deliver digital ads to those individuals most likely to respond. For companies in the telecommunications and media space, this is relevant both for their own marketing and as a facilitator of targeted marketing solutions. For example, Sky is testing "AdSmart" in the UK as a solution that target ads within Sky programming playing through set-top boxes and on mobile screens.[14]

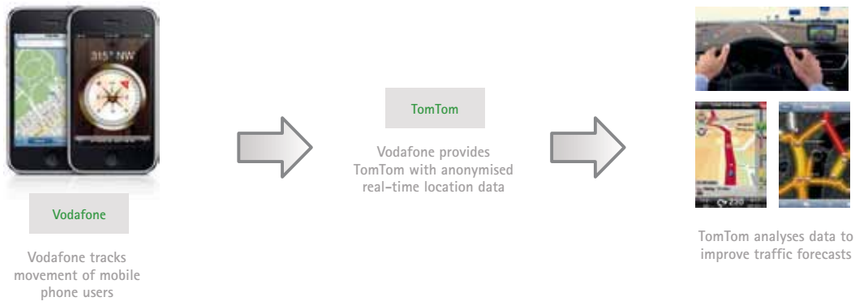
On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

[12] Source: Netflix's own tech blog, 6 April 2012

[13] Launch announced by Telefónica in October 2012

[14] Source: BSkyB; press

Secondary monetisation of location data



Source: Vodafone; TomTom

The benefits for organisations and consumers

Utilising insight generated from personal data to increase customer retention and reduce churn. By focusing on key "influencer" customers – those whom other customers tend to follow – telecommunications companies can more efficiently allocate their retention resourc-es. For example, Telekomunikacja Polska – the largest fixed network operator in Poland – analyses call records to understand social networks and identify prized "multipliers" within its customer base. Doing so has enabled it to improve the accuracy of its churn model by 47%[15]. (Whether an operator can take this approach will depend on country-specific telecommunication services laws.)

Enabling customers to opt in to location-based special offers from third parties. Leveraging the location data captured and transmitted by mobile devices on their networks, mobile telecommunications providers can offer third parties the ability to send highly relevant offers and deals to participating subscribers in real time. Case in point: Telefónica o_2 established its "Priority" programme in the UK to market event tickets and coupons to subscribers who opted in.

- Process automation reduces transaction costs for companies and improves customer satisfaction – which in turn boosts retention rates.
- Partnering with other sectors to create new data-driven services opens up new revenue streams – as does simply marketing the data, or insight derived from it, to third parties.

- Targeted advertising – especially when enhanced by real-time location data – maximises the company's own marketing investment. It can also mean additional revenue when the data is used by third parties to target their own ads and offers.

- Self-service anytime-anywhere transactions save consumers time, are more convenient than manual processes and improve the overall customer experience.

- Operational benefits achieved through efficiency improvements are partially passed on to consumers in the form of lower prices and enhanced services.

[15] Source: Sybase: "The Importance of Social Network Analysis," 2011

THE VALUE OF DIGITAL IDENTITY

SFR Régie – leveraging subscriber relationship and localisation data

Heightened competition and shrinking margins may be reining in growth in traditional telecommunications services, but for some providers, new opportunities lie, literally, in the palm of their hands. The increasing popularity and capabilities of smartphones, combined with the real-time location data that mobile carriers can so easily obtain, is spurring a host of new data applications. And that's spurring revenues.

The French mobile phone company SFR leverages its large customer base and its access to location data to offer companies a powerful way to target their marketing: send a deal or discount to a mobile subscriber based on where they are (walking near a restaurant, standing in a shopping mall, entering a department store and so on). The service – run through SFR's new mobile advertising arm, SFR Régie – is non-intrusive: Subscribers have to opt in to receive deals; and because the marketing is targeted, only relevant offers are made, so users aren't bombarded with unwanted advertisements.

So far, some 3.6 million SFR subscribers have opted in, receiving timely offers from SFR clients like Air France, McDonald's and Renault. This is just the beginning, too: As more telecommunications data – not just localisation info, but usage and status – is incorporated into efforts like SFR's, targeting should become even more specific, and effective.

5. Public services/health

- **The public services and health sector possesses large amounts of personal data, but relatively little of it has been digitised.**
- **It has more growth potential for organisational value than any other sector – largely due to the low-hanging fruit that awaits once digitisation efforts gain traction.**
- **Digital identity applications currently few and far between, with process automation being the initial focus.**
- **The euro crisis has given European governments an incentive to increase efficiency, jump-starting eGov initiatives.**
- **Some advanced, if still early-on applications – such as tax fraud detection and personalised medicine – demonstrate the high-value potential that can be realised.**

State of the sector

Without question, the public services and health sector came late to the digital identity party – and by some measures, it still has yet to arrive. While organisations possess vast amounts of personal data, the majority of it remains in paper form. Moreover, there have traditionally been few incentives to digitise data and boost efficiency. Public entities face little competition, and in the health care arena, the complex relationship between providers and payors, along with the sector's compensation schemes, means that the party that collects the information isn't always the one to benefit from its use.

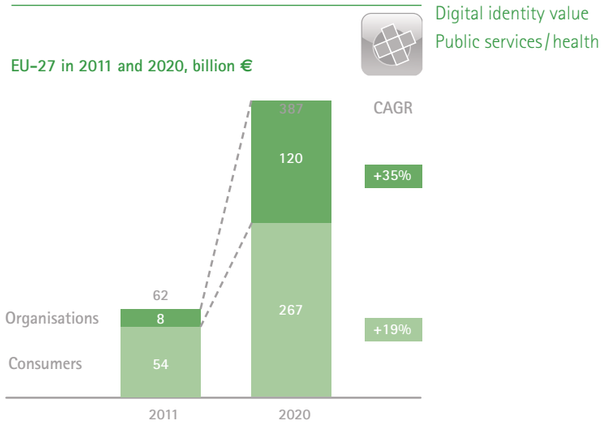
Key personal data applications
Public services/health

Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

The picture is starting to change, though. The euro crisis has spurred governments to boost efficiency, jump-starting eGov and citizen self-service initiatives. Meanwhile, the increasing use, and advancement, of IT in health care, combined with competition and pressure to cut costs, has led to more digitisation and the development of several very promising digital identity applications. To be sure, the public sector still lags behind all others, but it is, gradually, starting to gain ground.

The slow start means that there is plenty of low-hanging fruit. This and the sector's sheer size[16] explains why there is more growth potential for organisational value here than in any

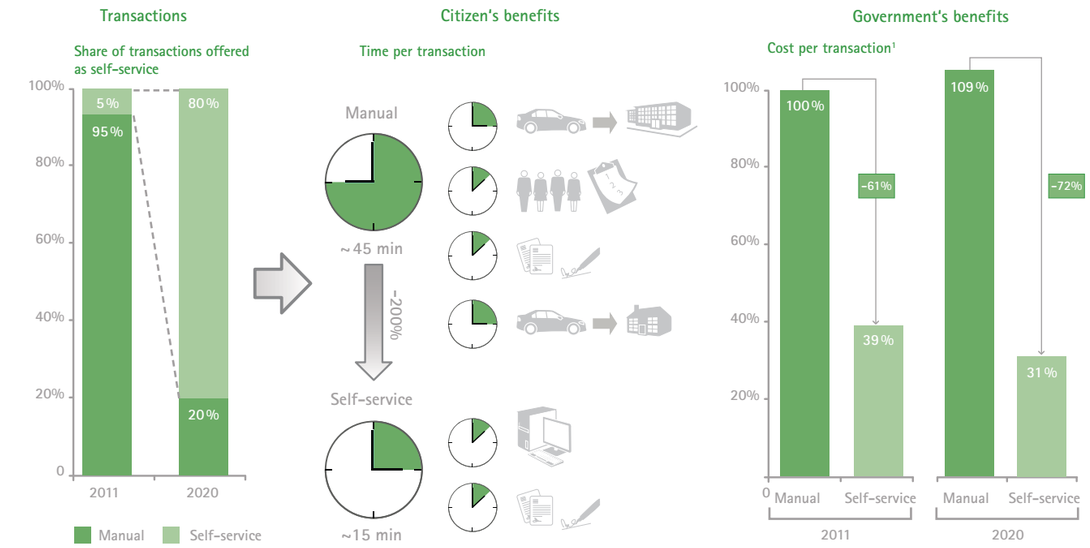
Digital identity value
Public services/health



Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

THE VALUE OF DIGITAL IDENTITY

Citizen self-service



Source: BCG analysis

other sector. Process automation is currently the major value contributor, but emerging uses, like personalised medicine, hold vast potential – not just to improve efficiency, but lives.

Key applications of digital identity

- **Citizen self-service:** Automated transactions – facilitated by secure digital authentication of citizens – provide a more convenient, more efficient alternative to traditional manual processes. A vast array of transactions – everything from reporting stolen bicycles to obtaining marriage licenses – can be, and increasingly are, performed via self-service. Denmark, a global leader in eGov, expects that nearly 80% of municipal transactions will be digital by 2015 and already generates €200 million in annual savings with electronic invoicing alone.[17]

Like banking and telecommunications, the public sector is rich in standardised, high-volume transactions – the kind ideally suited for customer, or in this case citizen, self-service. Examples abound: applying for a birth certificate, renewing a driver's license, registering a new address. Indeed, BCG estimates that by 2020, 80% of all public administration transactions could be offered as self-service in the EU-27 countries. They cost less to perform than manual transactions – coming in at roughly 40% the cost today, and dropping to less than 30% by the next decade. The cost efficiency is driven by replacing labour costs that tend to increase at the rate of inflation with IT software and hardware costs that are scaling. Self-service transactions are also far more convenient for many people, with no more waits on long lines. In the illustrative example outline above, what used to take 45 minutes of legwork now takes 15 minutes at a PC.

So far, however, public agencies in Europe – unlike their private-sector counterparts – have been slow to embrace these solutions. We estimate that in 2011 just five percent of all transactions were completed via self-service. That's costing governments more money and citizens more time than either should be spending.

- **Process automation – public services:** Public agencies can use digital data to automate decision making and processes. For instance, algorithms based on the personal data of job centre clients can be used to identify the best-suited professional training programme and thereby support the decision making of job centre employees to enable more efficient use of the public funds.

- **Process automation health care:** By making patient data more easily available to health care professionals, process flows, patient care and research can all be improved. Collection of data via mobile devices further increases the volume, data types and timeliness of the available information. An example of how this works can be found within the government-funded Swedish health care system. It allows for health data – including diagnoses, prescriptions, and full medical reports – to be accessed by a variety of stakeholders. A unique personal identity number enables reliable identification of each patient while ensuring data protection.

- **Personalised medicine:** By collecting and analysing a comprehensive, up-to-date array of patient data, customised health care is facilitated, with treatment focusing not just a presenting condition but the patient's overall situation. A leading example of this is Kaiser Permanente's personalised medicine initiative. Among the industry's most advanced data users, the U.S.-based health care payor/provider captures a broad collection of medical records, from hospitals, medical offices, labs and pharmacies, analysing them as a set to focus treatment on the patient's total health.[18]

Applications using personal data promise to revolutionise medical treatment and deliver significant cost savings. But realising the full potential of personalised medicine, decision support systems and other tools that leverage digital identity will require a health care setting where IT is utilised broadly – and effectively. Is Europe there yet? BCG's Health Care IT Score was designed to indicate how well a country's health care system is prepared to reap digital identity value.

The results show two things clearly. First, the starting position is very different from country to country and the focus areas to advance IT in health care differ as well. Secondly, all European nations have room for improvement.

[16] More than 50% of all eight sectors combined. See appendix for a detailed breakdown of sector sizes.

[17] Source: Case study "eInvoicing in Denmark," 2007; press

[18] Among the prominent examples of how Kaiser Permanente's rich data sets were applied is when Merck had to pull blockbuster medication Vioxx from the market in 2004, after a study based on Kaiser Permanente data provided proof of Vioxx' comparatively high risks.

THE VALUE OF DIGITAL IDENTITY

Maturity of IT utilisation in European health care

Scores represent absolute maturity, whereas 1 is the lowest maturity score and 5 is the highest maturity score, 2012

[1] Rounded average of maturity scores from rating elements
Source: BCG analysis

- **Tax collection:** To help detect tax fraud, personal data – such as bank records and credit card statements – is analysed and compared with disclosed information. Italy recovered €11.5 billion in 2011 by thwarting tax evasion. It uses a system called "Redditometro" that analyses some 100 life-style indicators, including gym memberships and private school tuition, to optimise tax audits. The system assigns taxpayers scores for their risk of evasion, so that audits can focus on highest-risk individuals.[19]

On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

- **Automated medical decision support.** These systems, like the one under development by IBM and the US insurance company Wellpoint, analyse huge volumes of data from many sources – including patient records, research papers, medical textbooks, and population health data – to detect disease and suggest treatment options. As no medical doctor, especially general practitioners, can keep up with the latest research and advancements in diagnosis and treatment, such solutions can lead to many more patients benefitting from optimal care.

- **Further personalising medical treatment by taking behavioural and genetic data into account.** By collecting data on an individual's own DNA, companies like 23andMe aim to generate new insights to help guide treatment. Other companies, for instance the online portal PatientsLikeMe, contribute to adding richer data by involving patients more directly.

[19] Sources: Republic of Italy; The International Herald Tribune, 7 February 2012

The benefits for organisations and consumers

- Citizen self-service reduces costs per transaction significantly. Meanwhile, individuals save time – they no longer need to travel to and wait at public agency offices.

- Analysing data to crack down on tax evasion and fraud boosts government revenues.

- Personalised medicine and other data-driven health care improvements can result in more effective patient treatment, better outcomes and longer life expectancy. They can also help to cut health care costs.

Five major personal data applications in health care

Personal data application	Description
Proactive care	Utilise personal data to actively monitor and prepare health care visit, not only during visit but also before visit to prepare patient and after visit to give patient further instructions *Example: Sending an e-mail to a patient after a visit, including a summary, relevant educational health material and follow-up appointments*
Decision support systems	Utilise big data capabilities to analyse digitalised medical records and medical knowledge databases to support doctors in diagnosis and treatment process *Example: Wellpoint and IBM developing a system based on the powerful AI unit "Watson" with the goal to provide up-to-date, evidence-based and individualised health care*
Personalised medicine	Base treatment of patients not only on diagnostics, but also on more comprehensive personal data, e.g., genetic characteristics, behavioural data *Example: Analysing genetic data and medical record of patient to predict chances of future illness and recommend preventive actions based on patient's behaviour*
Process automation	Utilise technological capacities to automate services, i.e., telemedicine for video sessions and diagnostics, where only basic information such as heart rate, blood pressure etc. is required *Example: Reducing hospitalisation time through telemonitoring older persons and those in high-risk groups after a heart attack through digital blood pressure and heart rate checks via face-to-face video conferences*
Enhanced R&D	Extract insight from personal data analysis to align R&D goals with regard to a more personalised approach for each patient rather than "one-size-fits-all" medicine *Example: Develop more comprehensive ways to analyse the genetic data to support the development of more effective medicine, with a more preventive rather than reactive focus*

THE VALUE OF DIGITAL IDENTITY

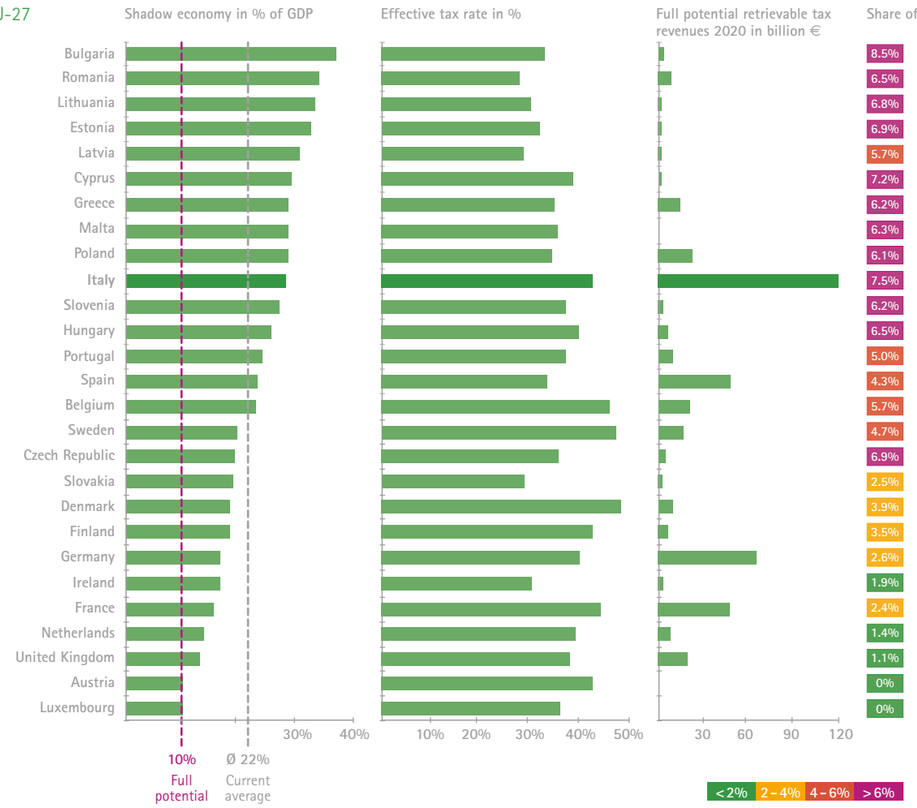
- The sale of personal information that is unique to the public sector – such as motor vehicle data useful to insurance companies[20] – can provide a minor source of additional income, but needs to be carefully balanced against the potential loss of trust citizens have in their states regarding their data.

- All operational benefits from public-sector digital identity use will be handed back to consumers through lower taxes or improved public services.

- The major part of savings achieved through personal data use in health care will also be handed back to consumers in the form of lower prices and health insurance premiums.

The shadow economy – in which goods and services are paid for in cash without any tax collected – is a problem for all countries, but particularly within the EU-27, where it averages 22% of each nation's GDP (for comparison, the rate is 9% for the United States and 11% for Japan). This translates into many billions of Euros in lost government revenues.

Retrievable tax revenues of shadow economy in EU-27



Source: Tax Justice Network "The Cost of Tax Abuse," 2011; Dr. Friedrich Schneider: "The Shadow Economy in Europe," 2009; BCG analysis

Digital identity applications offer a means to stem those losses and lessen the crushing pressure governments are under – more so since the euro crisis – to realise savings. BCG considers a reduction of the shadow economy to 10% of GDP as fully attainable by 2020.

Doing so will take a combination of innovative measures, such as automated tax collection and the analysis of tax and bank data to identify, and discourage, potential tax evasion. Already we are seeing some important first steps leveraging personal data. Germany has introduced a standardised tax ID to trace tax collections more effectively and create more transparency, with the goal of making tax fraud more difficult. The EU is currently discussing the implementation of a similar approach across all its member states.

Much more will be needed, but the combination of technological advances and incentives – both increasingly rapidly – will drive progress, drawing more tax revenue out of the shadow economies.

Italy – fighting tax evasion with "Redditometro"

Italy has the dubious distinction of probably losing more revenue through tax evasion than any other European nation. Little wonder, then, that it is now taking the most aggressive, and innovative, measures to combat the problem. Italy's automated system to detect potential tax fraud – "Redditometro" – collects data from financial institutions, public agencies and other organisations to infer an individual's standard of living based on more than 100 indicators (such as home mortgages, school tuition payments, car ownership and gym memberships). That standard is compared to the citizen's declared tax amount (in Italy, filing tax declarations online is mandatory), and instances of potential fraud are flagged for further investigation.

Redditometro results in a much more effective auditing process – focusing not on a random sampling of tax filings, but on those most likely to actually involve some degree of tax evasion. The system's success has been dramatic: Italy recovered €11.5 billion in 2011. This figure is expected to further improve over the coming years as the system is optimised and more data types are added.

IBM and Wellpoint – automated medical decision support system

Medical care can also benefit from aggregating and interpreting large collections of data. Doctors, after all, make diagnoses and develop treatment options not just according to their examination of a patient,

[20] In 2011, French government passed a law, enabling it to sell license plate data to commercial companies. The data is currently offered for €0.087 and €0.200 per record according to purchased volume.

but on that individual's medical history, along with the latest research on conditions and care. A new system from IBM and Wellpoint can guide them to the right conclusion by finding and analysing the relevant data with lightning speed.

Based on IBM's powerful analytical engine, "Watson," the system uses data from various sources – including patient medical records, treatment and claim history, research papers and medical textbooks (all increasingly available in digital form) – to detect likely diseases and injuries and provide treatment options. It considers possible drug interactions when suggesting medicine use, and even looks at national databases on disease outbreaks to inform its judgement. Precise responses are provided in less than three seconds. The result is up-to-date, evidence-based, individualised health care – and a way to cut costs while improving treatment.

Systems like these do face challenges, however. Providers may be hesitant to invest in the technology if only insurance companies benefit from the cost savings. There may be legal restrictions on using certain types of medical data. And there are medical doctors who need to adopt their practices.

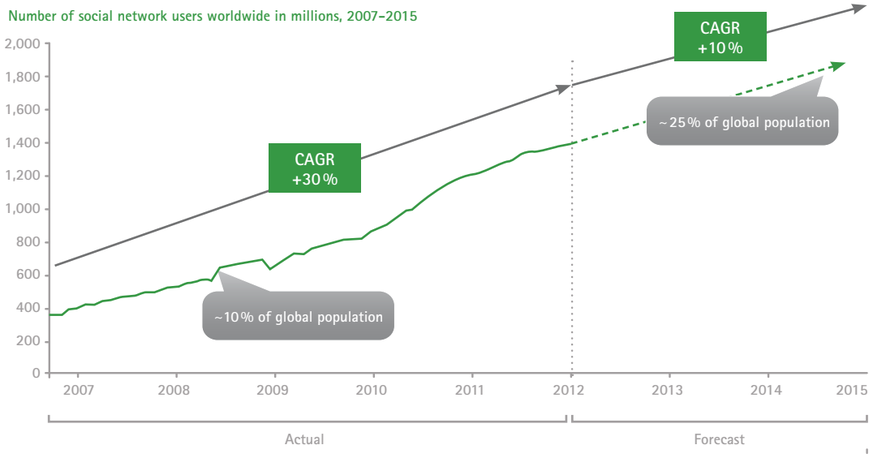
6. Web 2.0 communities

- **Personal data – created and shared by users – is the primary asset.**
- **The types of content generated by Web 2.0 communities are wide-ranging and detailed: demographics, employment and education data, interests, family and social connections, photos, videos, product feedback and location data – to name a few.**
- **Data volume and types will increase as social media continues its strong growth and mobile applications enable users to spend more time using these services.**
- **Targeted marketing and other ways to monetise the user-generated content are currently the main applications.**
- **Integration of a social component on other websites, blogs and services is increasing and could spur a host of innovative – and potentially lucrative – applications.**

Social networks are enjoying rapid – and widespread – growth. In the United Kingdom, approximately 60% of the population is on Facebook; in Iceland the figure is around 70%. The strong growth will continue throughout the world. By 2015, a quarter of the globe's citizens will have joined a social network.

Social media is already a fertile source of personal data, including interests, educational and professional histories, preferences, places visited, activities performed and milestones in one's life.

Global growth of social networks



Source: Morgan Stanley research; Strategy Analytics research; eMarketer; UN "World Population Forecast"; BCG analysis

All of this can be – and is – used to generate consumer insight and target marketing. More data types are coming (imagine paying with a phone-based digital wallet and having the purchase posted directly on Facebook). Companies already use social media data to focus research efforts, understand customer interests and know which discounts to send which users.

There's also the participatory aspect of the social Web. Dialogues with customers, and surveys to gauge interests and gain feedback (and even new product ideas) happen in real-time. That gives customers a potent voice in how products are developed and supported, it lets companies better serve them and it builds stronger, more lasting, relationships.

State of the sector

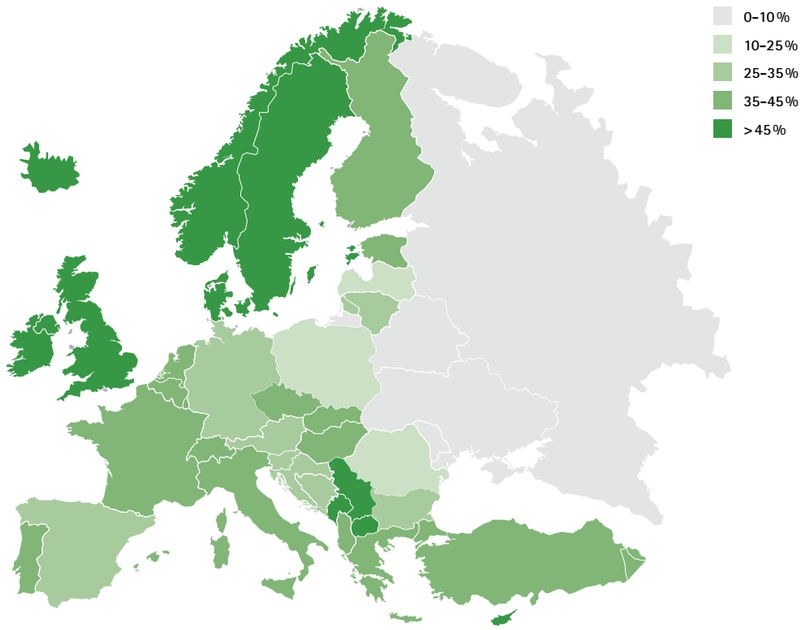
Personal data is the main asset of social and professional networks like Facebook, LinkedIn and XING. These sites exist, after all, to give users a platform on which to create and share content – not just details like employment, education and interests, but photos, video clips, social connections and location information.

Web 2.0 communities are starting to purse a range of digital identity applications. Among them: partnering with other sectors to add a social component to existing services; and monetising the insight gleaned from user data. But for now, at least, the main focus is on targeted marketing and other ways to monetise the user-generated content. The profiling of users is not only used for targeting advertisements, but is a

THE VALUE OF DIGITAL IDENTITY

Facebook penetration in Europe

Facebook users as share of country population, 2012



Source: Socialbakers, July 2012; BCG analysis

substantial element in improving the user experience and increasing usage; for instance, through recommending new connections and providing more relevant news and updates.

Key applications of digital identity

- **Service enhancements:** User data is applied to develop a personalised product experience for the network members. Based on profiles and the derived preferences, users receive recommendations on whom to connect or what to see, listen and read. Thus, the social and professional networks strengthen their customers' loyalty and increase the time spent on the site.

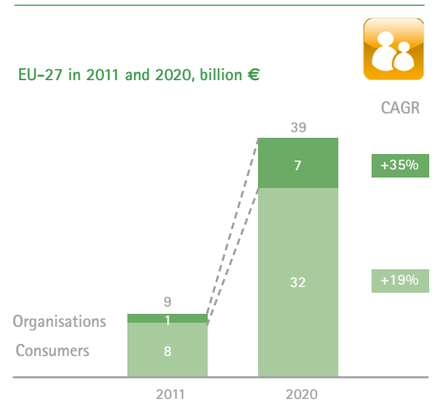
- **Monetisation of user-generated content:** The insight generated from highly detailed user content – or simply the data itself – can be marketed to third parties. A social network for professionals, for example, can generate valuable competitive intelligence for employers and recruiters. Monetising data and insight decreases the dependency of Web 2.0 communities on advertising revenue.

- **Targeted marketing:** Targeting is especially important for social networks as otherwise the ad inventory would be of very low value for advertisers. Facebook, for example, offers a broad range of criteria by which advertisers can target consumers, including geography, demographics, education level and user-defined "likes" (a popular Facebook feature which enables users to tag products and other things that interest them).

Key personal data applications Web 2.0 communities

Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

Digital identity value Web 2.0 communities



Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

THE VALUE OF DIGITAL IDENTITY

- **Default identity provider:** Increasingly, social media accounts are being used as a single sign-on to access a wide-range of external sites and services. Using their Facebook login, for example, users can sign on to a wide range of websites and even see who in their social network has also visited the site and what they may have done there (such as reading or sharing an article). This can greatly extend the reach of the social network.

On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

- **Development of more comprehensive mining techniques to generate insight from social networks and predict future trends.** Fashion designers, for example, have been able to detect nascent apparel trends more accurately based on insight inferred from photos, comments and location data generated by social networks.

- **Expanding into ad management platforms on third-party websites.** Increasingly, Web 2.0 communities are leveraging their user profiles to enable targeted advertising on third-party sites as well as their own. This is facilitated by the use of social media accounts as a single login and widgets integrated on third-party websites. Users are recognised on the external site and ads can be targeted accordingly.

The benefits for organisations and consumers

- Targeted advertising – on its own site and on third-party sites – will become increasingly effective as the user base and available data grow.

- Secondary monetisation of data or the insight derived from it can provide additional revenue streams.

- The use of a social media account as a default identity on the Web and for mobile applications increases customer loyalty and retention.

- Consumers gain – at no financial cost – a platform on which to represent themselves, share content, communicate with friends and family and network with professional contacts.

- The consumer surplus far exceeds the revenue that social and professional networks generate. According to a BCG report published in 2012, the consumer surplus of Internet services – including social networking – averages €2,900 annually per capita in Germany.[21]

As different forms of media gain, and lose, popularity, advertising spending adjusts, following the media usage of consumers. The process doesn't happen overnight, though. Advertisers and publishers need time to discover the optimal marketing applications and tactics for each new media channel. What we are seeing now is their steady shift from traditional advertising hotspots like print and radio to new ones like online (via desktops and laptops) and mobile (via smartphones and tablets).

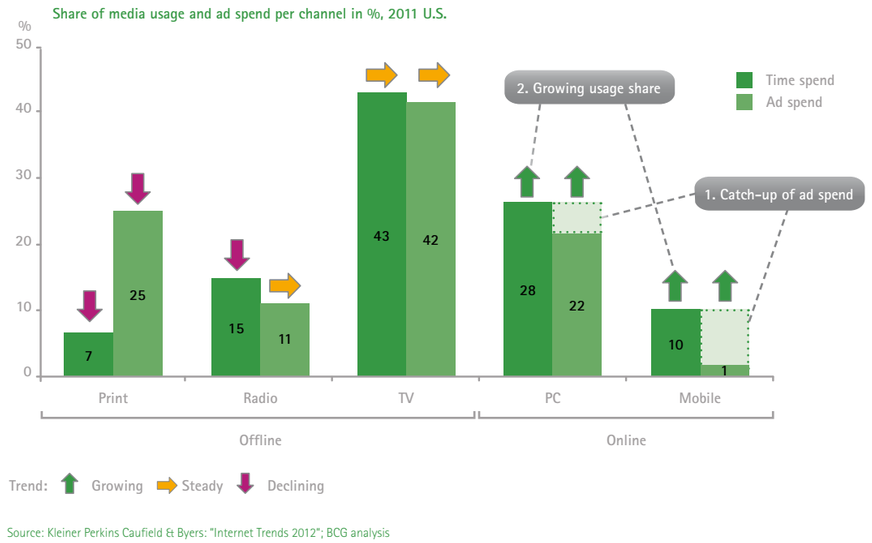
While advertising spending has nearly caught up with media usage for PC-based online channels, the "catch-up" process is just beginning for mobile devices. The steadily increasing penetration and usage of online media will contribute to a continued growth in online ad spend.

As they pursue new forms of revenue, social networks might want to take a cue from Google. Leveraging its superior know-how in capturing the content, and context, of websites, Google has developed an advertising business that now accounts for 96% of its revenue.[22] In the process, it has become a key platform for managing ads on third-party sites, using its technology to match online advertisements with the best-suited inventory.

Social media sites could follow a similar route. While they are already using the user profiles and personal data they possess to target personalised ads on their own sites, significant potential lies also on third-party websites. Already, many of these sites are implementing Web 2.0 community widgets, such as "like" and "share" buttons, enabling social networks to expand their reach on the Web and more extensively track their users' online behaviour. The insight they gain, combined with the targeting capabilities they employ on their own sites, could be employed to match ads with third-party inventory.

Going forward, advertisers and publishers will very likely find themselves with three main options in targeting online ads: Google's context-based targeting; social networks' targeting based on detailed user profiles; and third-party targeting platforms (like AudienceScience and nugg.ad). For them, a sound strategy is to try all three and closely follow and track campaigns, determining which route delivers the most efficient results in different settings.

Media usage and ad spend development



Source: Kleiner Perkins Caufield & Byers: "Internet Trends 2012"; BCG analysis

[21] BCG: "The Internet Economy in the G-20," March 2012; BCG's "Connected World" reports

[22] Source: Google 2011 annual report

7. E-commerce

- **Sector already makes extensive use of personal data.**
- **Recommendations, the major data-driven application, are responsible for up to 25% of revenue at best-of-breed sites.**
- **The most advanced sector in its use of targeted advertisements.**
- **The growth of mobile devices and social media sites bodes well for e-commerce companies, creating more touch points with consumers and more possibilities for innovative applications.**

State of the sector

The e-commerce sector – which depends on personal data to operate – makes pervasive, and sophisticated, use of digital personal information. It is the most advanced sector regarding the use of targeted ads, and its primary digital identity application – leveraging data to generate recommendations – is already a proven value driver. Indeed, one of the sector's leaders, Amazon, is expected to see up to 25% of its revenue triggered by its recommendations system, which steers consumers to items they might like based on profiles developed from past purchases and other data. Improving recommendations engines will continue to be a sector focus, and average performance will get closer to today's best in class.

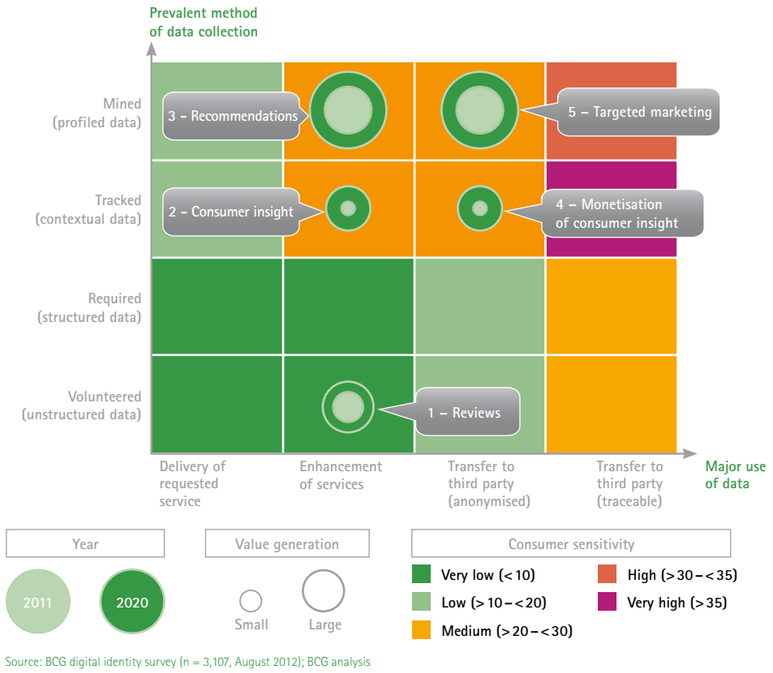
User-generated content – largely in the form of reviews – is also an important source of data. Not only does it influence purchasing decisions, but it is starting to be leveraged in other ways: analysed for insight that can improve internal processes, or monetised in sale to third parties.

The social media boom is creating more customer touch points, and the intensified usage of mobile apps means more traffic to e-commerce sites. Mobile devices, in particular, hold vast potential for the sector. Location information can be used to send offers at opportune times (such as when a consumer is in a brick-and-mortar store); apps can enable consumers to scan or photograph an in-store item and immediately receive a better price online. Among the different sectors, e-commerce has been, arguably, the most proactive in leveraging digital data. Advances in technology and the social Web will hand it new opportunities to do even more.

Key applications of digital identity

- **Reviews:** By encouraging and publishing user-created product reviews, e-commerce sites leverage the trust customers have in each other's experiences to drive sales. The more sophisticated systems allow customers to comment on individual reviews, creating a dialogue among users that fosters even more trust.
- **Consumer insight:** Usage and purchasing data is continuously analysed to derive insight for demand planning and offer design. Being able to align inventory closely with demand and recognising trends early are critical success factors in the competition within the e-commerce sector and with offline retailers.

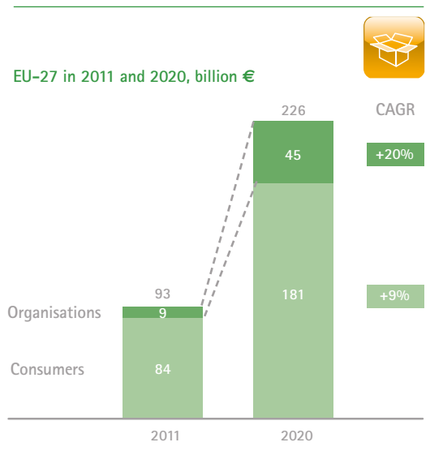
Key personal data applications
E-commerce



Source: BCG digital identity survey (n = 3,107, August 2012); BCG analysis

- **Recommendations:** Analysing a comprehensive set of consumer data – such as past purchases, products viewed and other users' purchases – e-commerce merchants generate relevant, user-specific recommendations that increase sales.
- **Monetisation of consumer insight:** The data generated by or about customers – and the insight derived from it – is often valuable to third parties (such as consumer goods manufacturers), and its sale can provide an additional revenue stream.

Digital identity value
E-commerce



Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

THE VALUE OF DIGITAL IDENTITY

- **Targeted marketing:** E-commerce sites are advanced users of targeted ads, employing them to drive more traffic to their sites and to improve conversion rates.

On the cutting edge – where applications may be more sophisticated and intriguing, but their prospects are more uncertain – we have observed the following uses:

- **Integrating social features with e-commerce.** The rise of Web 2.0 communities has made it possible to incorporate a social aspect into purchasing decisions. Used imaginatively, these features can help drive sales. Levi's "Friends Store," for example, displays products that a visitor's friends liked – thereby leveraging the trust consumers have in people they know.

- **Extending reach into the offline world.** Using mobile apps, some e-commerce companies are finding innovative ways to create more touch points with customers and extend their reach into the offline world. Amazon, for instance, has developed an app that lets users scan products to compare prices. The idea is that a customer standing in a store will see a lower price on their phone and complete their purchase online.

The benefits for organisations and consumers

- Recommendations influence buying decisions and drive sales – up to 25% of revenue in Amazon's case.

- Targeted advertisements remain a key driver of highly cost-efficient customer acquisition, with some forms of targeting increasing efficiency by a factor of six.[23]

- Selling customer insight to third parties in other sectors opens up a new revenue stream for e-commerce companies.

- For consumers, e-commerce provides greater convenience than in-store transactions and enables the identification of the best available price.

- Recommendations generated by vendors guide consumers to products that interest them, while user reviews give them confidence in their purchasing decision.

Overview of targeting techniques – used stand-alone or in combination

- **Behavioural.** In this technique, a user's browsing behaviour is monitored via cookies, tracking the websites he visits and the content he clicks on. From this information a profile is created. For instance, a user reading regularly golf articles might be marked as having an interest in sports, an interest in golf, being male and earning an above-average income. This example also demonstrates a key weakness of this technique: If several individuals – family members, for example – are using the same computer, the profile becomes blurred.

- **Contextual.** This technique does not require personal profiling. Instead, the content of a website is analysed to determine the topics that are being addressed there, and ads matched to those topics are displayed. For example, on a blog page discussing sites seen during a trip to Barcelona, contextual targeting would most probably result in travel- and tourism-related ads appearing.

- **Geographical.** In this form of targeting, an audience is selected by location, which is derived either from an IP address (typically indicating country, region and city) or through data on a GPS-capable device. Ads are then targeted based on that location; for example, a national website would show ads from a local retailer only to users located in that retailer's city.

- **Registration-based.** Leveraging the information a user provided during the registration process, this form of targeting can be based on a wide range of data, including age, interests and home address. These offers and ads can be highly personalised, since they have a lot of personal data to work with. For example, registered users of an online retailer may receive a special discount offer on their birthday.

- **Retargeted.** Retargeting is used to display ads of products a user has recently viewed in an online shop but hasn't bought. For example, a user might look at sports shoes on a fashion retailer's website, but then leave the site without purchasing them. Retargeting techniques will then display ads for that specific pair of shoes at the news or weather site the user visits the next morning.

- **Technical.** Here ads are delivering based on technical specifications that the user's browser automatically transmits. These can include the used device, Internet connectivity speed, clock settings and browser version. For example, video ads would only be delivered to devices with a fast Internet connection, or special discounts for dinner would only be displayed during the evening, when people are most likely to be thinking about dinner.

- **Frequency capping.** This technique requires measuring how often a user is exposed to a particular ad. The number of times that user is shown the ad can then be restricted – for instance, to four times a day – in order to optimise efficiency and minimise annoyance.

[23] Criteo claims such improvement over standard banner ads backed by joint study conducted with Nielsen in 2010.

THE VALUE OF DIGITAL IDENTITY

8. Online info/entertainment

- **Targeted advertising and recommendations are the major applications of digital data.**
- **The increasing use of mobile and Internet-ready devices is expanding the sector's reach and the data it generates.**
- **As users shift to online media for news and entertainment, advertisers are shifting as well, enhancing revenue opportunities.**
- **Incorporation of social media into services will enable increased personalisation of services.**

State of the sector

Smartphones, tablets, Internet-ready televisions and other connected devices have given online information and entertainment services more reach than ever – and as more users shift to online media for their news, video and music, more advertisers are shifting with them. The result for the sector is a confluence of good tidings: more users, generating more data, enhancing targeting capabilities sought out by more advertisers. Indeed, the major current value derived from personal data is targeted advertising.

The sector's other key application – especially important for entertainment services – is recommendations. Using systems that analyse different types of data, such as previous selections by a user and selections made by others, highly relevant suggestions can be made. That not only improves content navigation but also increases usage time and up-selling.

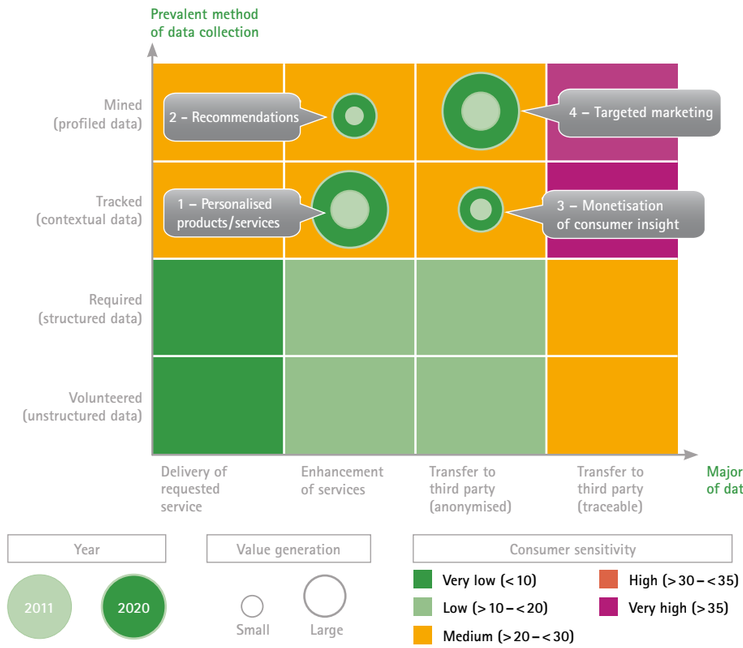
Meanwhile, personalised services – often offered on a subscription basis – and secondary monetisation (selling data or insight derived from it to third parties) both offer growing revenue streams that the sector is starting to pursue. The integration of a social component in services – via partnerships with Web 2.0 communities – presents opportunities for further personalisation, enhanced customer experiences and new data-driven applications.

Key applications of digital identity

- **Personalised products/services:** By using personal data to infer the interests of users, content can be customised for them. These personalised services can be monetised through subscription fees or advertisements. Spotify, for example, will individually stream a user's preferred music whenever it is connected to the Internet.
- **Recommendations:** By analysing a variety of data sources, entertainment choices that accurately reflect a user's interests can be suggested. These recommendations, in turn, can improve content navigation, increase usage time and boost up-selling. A well-known example is YouTube's video recommendation system, which generates recommendations based on user profile, viewing history, ratings of content and other data sources.
- **Monetisation of consumer insight:** The data that information and entertainment services generate or collect from their customers can be highly valuable to third parties. Monetising this information – or the insight derived from it – creates an additional revenue source. Case in point: Twitter started syndicating its proprietary data to several resellers. Those companies, mainly start-ups, use the data to, among other things, capture the stock market sentiment.
- **Targeted marketing:** The personal data that is collected can be leveraged to deliver digital ads to narrowly defined target groups. Google, for example, collects a variety of data – demographics, preferences and browsing history, to name a few – in order to profile users. These profiles are then used to target advertising from third parties.

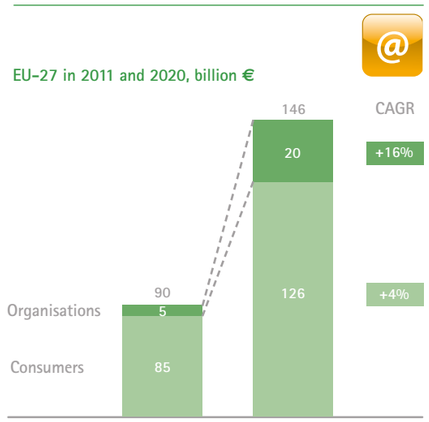
On the cutting edge – where applications may be more sophisticated and intriguing, but

Key personal data applications
Online info/entertainment



Source: BCG digital ientity survey (n = 3,107, August 2012)

Digital identity value
Online info/entertainment

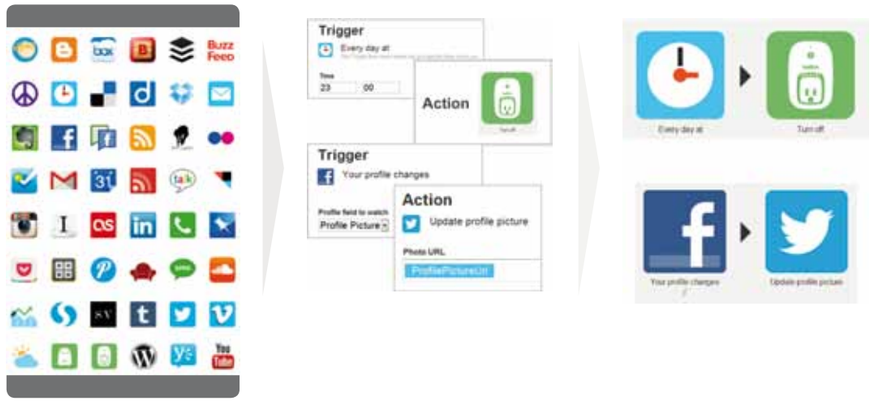


Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

THE VALUE OF DIGITAL IDENTITY

Innovative personalisation

IFTTT



Source: IFTTT

their prospects are more uncertain – we have observed the following uses:

- **Incorporating social media features in order to further personalise media consumption.** By now, many websites incorporate basic social features such as "like" and "share" widgets. Future differentiation depends on deeper and more natural ways of making info and entertainment services more social. For instance, Spotify incorporates features that allow users to access the playlists and favourite songs of their friends, and let them share their own music selections automatically on social media sites.

The world around us isn't just growing but becoming more interconnected. Today's communications technologies enable physical objects to transmit and receive data – creating a vast, and rapidly expanding, Internet of things. This opens up a wealth of possibilities, only some of which we are starting to realise now.

One such application is personalised automation that incorporates, and links, both Web services and "real world" components. IFTTT – "If This Then That" – is one interesting example of this kind of "blended" automation that serves as an outlook of things to come. Its premise is simple: Users set a trigger (the "this") that causes an action (the "that") to be taken. But the twist is that the trigger-action combinations – or recipes, as IFTTT calls them – can mix different services. So if a new Facebook friend is added (the "this"), a tweet about it can automatically be made (the "that"). IFTTT's first step was to integrate different Internet channels, but now it is expanding into physical applications, too. Recently, it added WeMo – a family of sensor and switch devices for home automation – to its list of channels. That means that now when a new Facebook friend is added, a light in the living room can turn on.

But it also means a lot more: a level of personalisation that is potentially boundless. Building bridges between the physical and digital worlds won't just bring convenience to users – but revenue to those who do it well.

The benefits for organisations and consumers

- Personalisation enhances the value of information and entertainment services – realised through either subscription fees or advertising.
- Selling collected and user-generated data to third parties provides an additional source of revenue.
- Customers benefit from access to vast content offerings at no, or for little, charge. Online info and entertainment services represent a major share of the large consumer surplus of Internet services.[24]
- Sophisticated, accurate recommendations systems allow users to more easily navigate services and find content they like.

Spotify – Integration of social media with wide range of privacy options for users

For entertainment sites, social media offers both potential and peril. Features that facilitate sharing – letting a user's friends see what he or she is interested in – are a powerful way to spread the word about a service, reach new audiences and build the user base. But they have to be implemented in a way that builds trust, too. Users may not want too much information shared, or shared with everyone. Privacy controls have to be available, intuitive and granular.

Balancing sharing with privacy is no simple task, but an interesting model for it is Spotify, the popular streaming music service. It is tightly integrated with social media; specifically, with Facebook. Users can share, automatically, information on songs they are currently listening to, or what they have listened to previously. Their favourite tunes and playlists can be accessed, too, by Facebook friends. This provides value to users, who get recommendations from people they trust – and to Spotify, which expands its reach.

But what makes that value sustainable is the way privacy is addressed. Spotify offers a range of options that give users very personalised, and very detailed, control over sharing. They can choose what playlists and favourites to share; whom to share with; and how much information gets posted. They can choose to enjoy private listening sessions, too, when they don't want their 600 best friends knowing just how much they enjoy Broadway musicals. Spotify's savvy use of social media features has helped spur a rapid growth in its subscribers.

[24] BCG: "The Internet Economy in the G-20," March 2012; BCG's "Connected World" reports

part 4

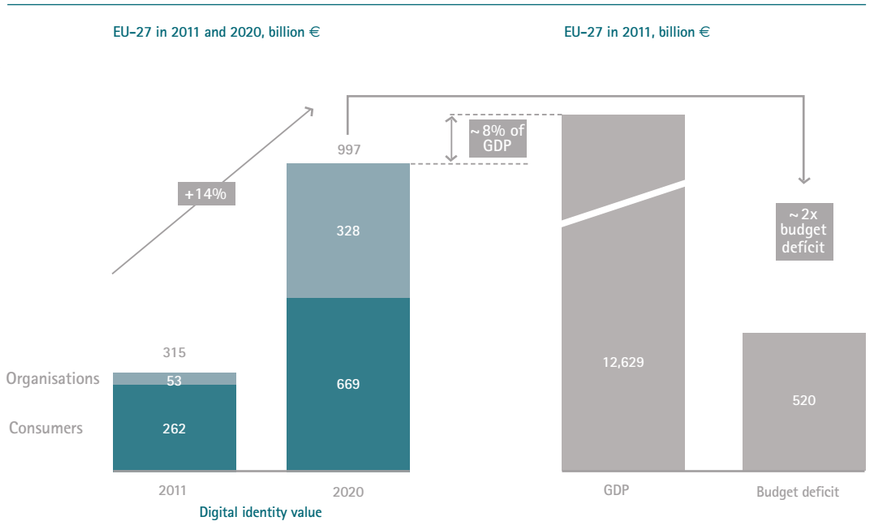
THE MEGATRENDS OF DIGITAL IDENTITY

THE MEGATRENDS OF DIGITAL IDENTITY

A growth driver for a stagnant economy

As detailed earlier in this report, many of the most common applications of personal data are currently only starting to tap their potential value. It is still too early to tell which of the emerging uses will succeed and what additional applications will be unveiled over the next decade. But one fact is clear: The opportunities digital identity offers are enormous. It can drive massive growth in an otherwise stagnant European economy, and the value it provides can amount to roughly 8% of EU-27 GDP by 2020 (see Exhibit below).

Digital identity value key driver of overall economy



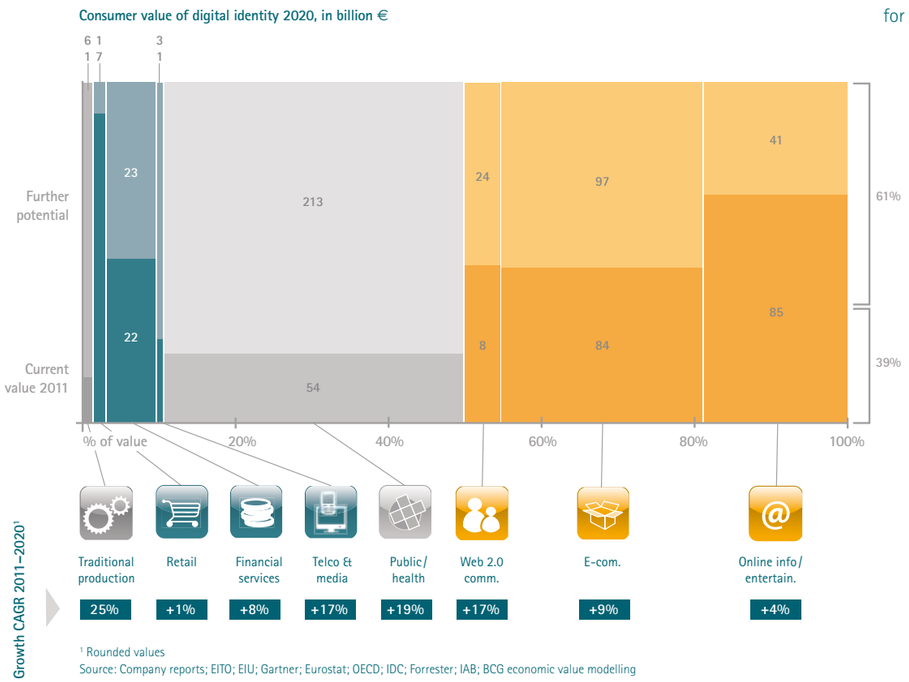
Source: OECD; BCG economic value modelling

Although the public debate on monetisation of personal data is dominated by the perspectives of Web 2.0 players and the digital economy, digital identity is not just the realm of the Facebooks and Googles of the world. It is relevant, and important, for the economy as a whole. In fact, it is the public sector and health care industry that stand to profit the most from personal data applications – potentially realising 40% of the total organisational benefit (as detailed in Exhibit *Digital identity value for organisations*). But these are not the only traditional sectors with strong growth prospects. Companies from the manufacturing, financial services, and telecommunications and media industries are expected to achieve digital identity value growth rates comparable to those of the Internet sector. This is due to a significant increase in digital identity intensity – the estimated share of digital identity value of the overall sector size – as the application of personal data will play a more and more important role in those sectors. This ratio is expected to remain relatively stable for Internet companies because they already make sophisticated and vast use of personal data. Growth in those sectors will be spurred mainly by an ongoing increase in Internet penetration of and usage by the European population. Although the extent to which digital identity is applied in the retail sector is at a similar level to that of Internet companies, this sector is expected to have only a modest growth rate because the retail sector will not grow as dynamically.

Public sector and health care industry stand to profit the most from personal data applications – potentially realising 40% of the total organisational benefit.

The benefits of digital identity are relevant and important for consumers as well. Indeed, we estimate that the consumer benefit will be

Digital identity value for consumers

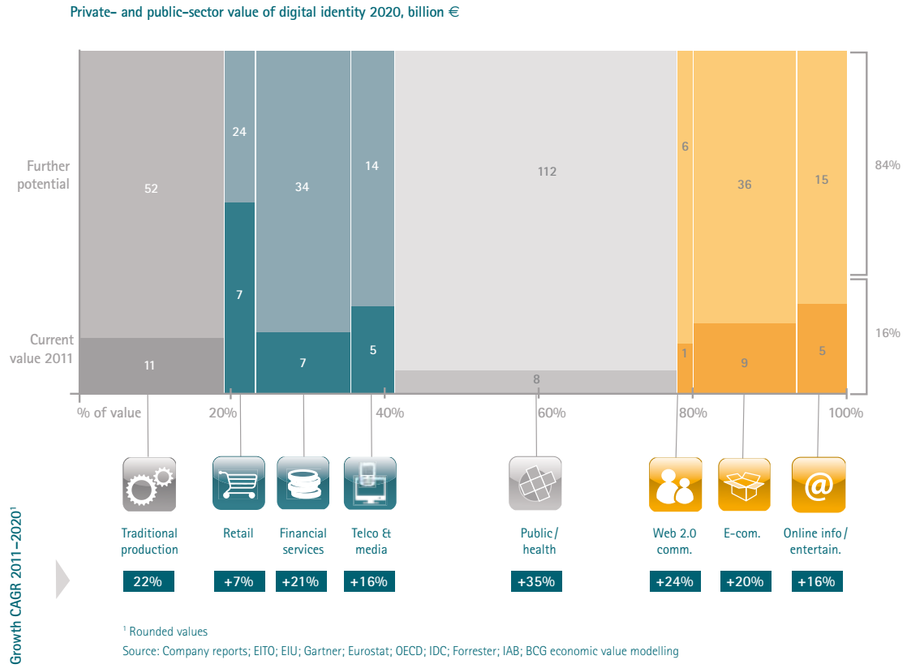


[1] Rounded values
Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

[1] See appendix "Development of digital identity intensity per sector" for details

THE MEGATRENDS

Digital identity value for organisations



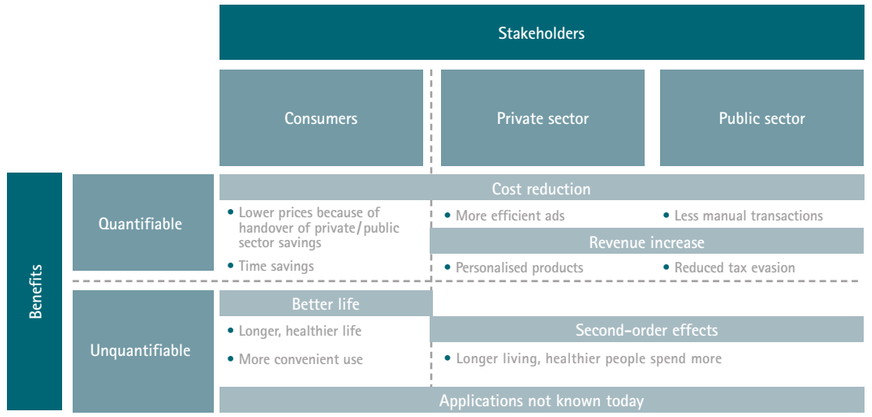
more than double the organisational value – €670 billion a year by 2020 – mainly stemming from reduced prices (passed on by companies seeing data-driven cost savings), the time savings that self-service and automated transactions will bring and the high value individuals place on free online services, supported at least in part by the use of personal data (as shown in Exhibit *Digital identity value for consumers*). The latter in particular is a source of tremendous consumer value created by Internet companies. The consumer surplus of Internet services – including social networking, online shopping, e-mail and online news – averages for instance about €2,900 annually per capita in Germany.[2] The equally large consumer value in the public and health care sectors results from the fact that most of the benefits achieved by those organisations will be passed on to citizens in the form of tax reductions or other savings.[3]

The total benefit of digital identity will likely be even higher than the €1 trillion in quantifiable benefits we anticipate by 2020. As shown in Exhibit *Overview of quantifiable and unquantifiable benefits of digital identity applications,* various unquantifiable benefits will be created as well, such as the longer lives individuals may enjoy and the greater conveniences

[2] BCG: "The Internet Economy in the G-20," March 2012; BCG's "Connected World" reports

[3] One notable exception is reduced tax evasion, which increases the fairness of taxation, but does not result in monetary benefits for citizens overall.

Overview of quantifiable and unquantifiable benefits of digital identity applications



they will see thanks to applications using personal data. Second-order effects will add to the total, too: People who live longer lives, for example, will spend more money. Finally, there are all the as yet unknown applications that will bear fruit as they inevitably enter the scene over the course of the next decade.

Sectors are at different stages of generating value from personal data

Part 3 shows in great detail how the various sectors make very different use of personal data. We summarise the stage a sector or single organisation is at in terms of its use of digital identity with the path depicted in Exhibit *Evolutionary path of digital identity value creation.*

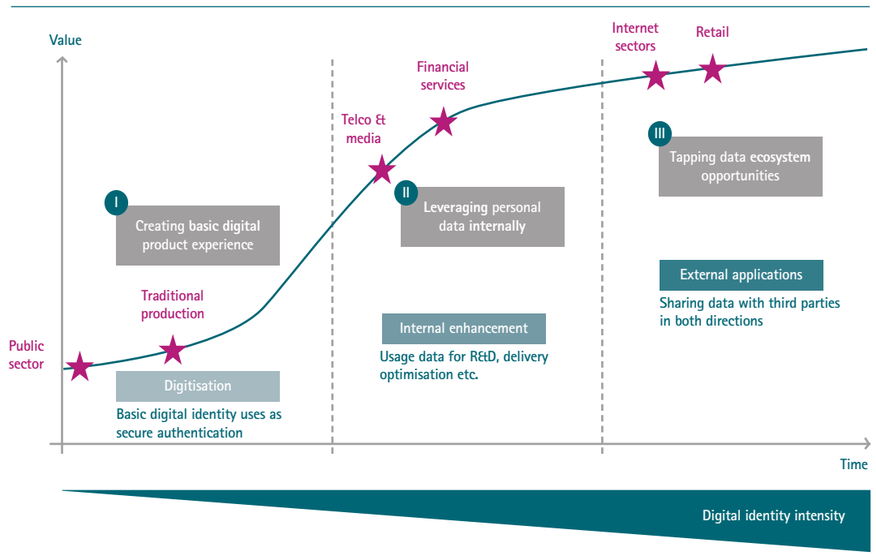
Retail and the three Internet sectors are already at a relatively advanced level; these organisations routinely leverage personal data internally for R&D to optimise the delivery of their goods and services and for other purposes. They often tap into the wider ecosystem of data-related opportunities as well, such as sharing – and selling – information to third parties.

Companies in the telecommunications and media sector, including cable operators, have access to a vast amount of personal data in principle – mainly relating to telephony and Internet usage or TV viewing – but so far make relatively little use of it. While customer self-service and process automation are currently the major applications of digital identity, we expect the focus to shift to innovative new services and enhanced user experience.

The traditional production and public sectors, meanwhile, are only at the very beginning of the path. Many of these organisations are only now starting to create a basic digital product experience or embrace digitisation – such as government agencies and health care providers migrating

THE MEGATRENDS

Evolutionary path of digital identity value creation



The traditional production and public sectors are at the very beginning of the path, only now starting to create a basic digital product experience or embrace digitisation.

to electronic records and setting up processes that leverage this data along the value chain.

The six key trends in digital identity applications

While the actual applications of personal information vary from sector to sector, and even from organisation to organisation, they invariably fall into one of six categories. These are the megatrends of digital identity that are relevant for organisations at each stage of the path:

- **Process automation.** By integrating personal data into their processes, organisations can automate – and simplify and speed up – transactions that traditionally required users to identify themselves, express their preferences or perform some kind of manual action.

One of the most common applications of automation is the online ordering process used by e-commerce sites. Billing and shipping information is collected once and stored; it is then used to prefill forms for subsequent purchases. This not only saves consumers time, but also prevents errors.

Increasingly, process automation can be found in the offline world as well. For example, the Oyster Card carried by London commuters authenticates them when they board buses and trains, automating ticketing and access control. Meanwhile, many products can store and apply user preferences – like an automobile that automatically adjusts the seat and mirrors to each driver's liking.

This is just the beginning. Emerging technologies like near-field communication – where users authorise payment simply by placing their smartphone near a reader – will spur all manner of automated processes.

- **User enablement.** Digital identity gives individuals the ability to perform transactions autonomously without any human assistance. Customer self-service is a prime example. It continues to grow strongly in sectors where it has been applied for decades – particularly in banking and the telecommunications industry – and is being introduced in more and more new industries. Its popularity is easy to understand: Consumers save time and effort, and organisations save money by replacing manual labour with IT solutions – and as labour costs increase and IT costs drop, the savings become even more significant. By passing on some of these savings in the form of reduced prices, companies can also leverage user enablement to gain a competitive advantage.

These types of applications are becoming a focal point of the public sector, as citizen self-service portals can simultaneously reduce budget pressure and increase efficiency. Denmark, for example, has one of the most advanced e-government programmes in the world and generates €200 million in annual savings with electronic invoicing alone.[4]

The most successful applications all share one vital trait: They provide a simple and intuitive user experience. As Jeff Bezos, founder and CEO of Amazon, puts it: "Every time a customer contacts us, we see it as a defect."[5]

- **Personalisation.** Customising products and services to a particular individual's preferences and needs makes them more relevant to that person. That spurs sales for the organisation and satisfaction for the consumer. Traditionally, personalised products came about through bespoke solutions at high cost premiums and for small target audiences. Digital identity enables personalisation on a widescale, cost-effective basis (due to the availability of more data and improved processing power).

Online retailers leverage a user's purchase and browsing history to generate personalised recommendations and custom storefronts – featuring products relevant to each individual consumer. When executed well, these applications can create great value: Amazon's recommendations, for example, are estimated to generate some 25% of the e-commerce giant's sales.

More traditional sectors, too, are discovering that data-driven personalisation can drive new offerings and enhance the appeal of those that already exist. Retailers can deliver coupons and offers by e-mail or mobile based on a customer's past purchases, browsing history or even their current location (the latter is made possible using the GPS capabilities of smartphones).

- **Enhanced delivery.** The availability of both more volume and more types of data enables organisations to increasingly extract operational insight from it. This allows them to improve the delivery of goods and services. For instance, IBM and the U.S. insurer Wellpoint are developing a system to analyse huge volumes of data from many sources – including research papers, medical textbooks and population health

[4] Source: Case study "eInvoicing in Denmark," 2007; press
[5] Wired Magazine online, 13 November 2011

THE MEGATRENDS

data – to detect diseases and suggest treatment options. Such solutions can lead to many more patients benefiting from optimal care.

Different industries are at different stages in leveraging data to enhance delivery, and not surprisingly, the online sector is currently ahead. But even in the public sector, the opportunities are rich: Applications are starting to emerge that can fight tax evasion and fraud in government programmes. Health care, too, stands to reap substantial benefits from enhanced delivery, with the insight gleaned from vast data sets leading to more effective patient treatment.

- **Personal data-driven R&D.** Using a range of data sources – such as product reviews, comments posted on social media sites and usage data from in-product sensors – companies can also gain insights that let them better focus their research efforts and shorten development cycles. This trend has already been adopted by major consumer goods companies, including Procter & Gamble, whose Vocalpoint P&G community gets customers more deeply involved in the development and testing of new products.

  Using personal data to drive R&D is a particularly compelling proposition for traditional industries where, historically, little usage data has been available and consumer research can be expensive – much more so than in other sectors such as the Internet and software industries.

- **Secondary monetisation.** The data that an organisation holds and the insight derived from it is valuable to other parties – valuable enough that marketing it can open up a significant new revenue stream. This is highly relevant for any organisation that has access to a proprietary data set and user consent for third-party application of the personal information or sufficiently anonymized data.

For instance, in the online sector, Twitter recently sold access to the billions of tweets its users openly publish through the service. Third-party companies syndicating this data use it, among other things, to capture the stock market sentiment.

Even the public sector has tried to monetise its personal data. In the United States, the state of Oklahoma realises about $13 million annually by selling information it collects from drivers. This and similar European examples of secondary monetisation raise questions about the balance of the expected return and the potential loss of citizens' trust. Is it worth it to market such data without the explicit consent of the individuals for a few million euro when there are applications of personal data worth billions of euro that require citizens' trust and collaboration?

So how can organisations and policy makers unlock the value potential of digital identity? In the following part 5, we present a new paradigm for responsible application of personal data – in a sustainable, consumer-centred way – and offer guiding principles for key stakeholders.

Is it worth it to market such data without the explicit consent of the individuals for a few million euro when there are applications of personal data worth billions of euro that require citizens' trust and collaboration?

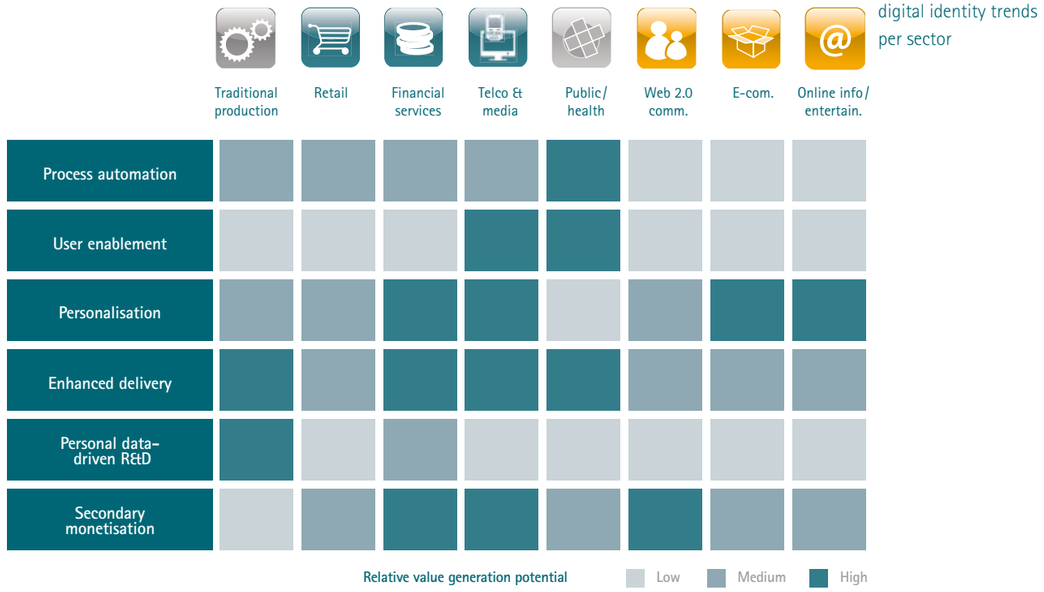
[6] Source: NIC Inc. website; Oklahoma State Budget; Oklahoma Tax Commission website

[7] In 2011, the French government passed a law enabling it to sell license plate data to commercial companies. The data is currently offered for a price of €0.087 to €0.200 per record, depending on the purchased volume.

Key trends of digital identity value creation

Key trends	Description
Process automation	Applying digital identity of users to automate processes as users do not have to identify themselves and preferences are known as part of the profile
User enablement	Empowering users to perform transactions autonomously without any need for a human counterpart
Personalisation	Providing more relevant products, services and advertisements based on knowledge about consumers that is available and processed in real-time
Enhanced delivery	Adding of new data sources to profiles and applying of big data capabilities to extract new insights to improve delivery of products and services
Personal data-driven R&D	Using new and combined data sources and big data analytics to increase R&D efficiency and effectiveness
Secondary monetisation	Exploring ways to sell personal data in anonymised or fully traceable form to third parties

Relative importance of digital identity trends per sector



part 5

A PRACTITIONER'S GUIDE TO THE FUTURE OF DIGITAL IDENTITY

A PRACTITIONER'S GUIDE

A PRACTITIONER'S GUIDE TO THE FUTURE OF DIGITAL IDENTITY

As detailed in the previous parts of the report, the opportunities presented by digital identity – when managed carefully – are enormous. But so, too, are the lost opportunities, should it not be handled in a thoughtful, balanced way. Our research shows that the latter scenario is all too possible. Today, consumers have a generally low awareness of how their personal information is being used; if that awareness should rise, it will likely result in a decreased willingness to share data – all else being equal. On the other hand, easy-to-use privacy options and controls can significantly increase that willingness to share. Anyone seeking to create value through digital identity needs to understand the implications of that dynamic. If consumers' awareness of data collection and use increases without organisations establishing practices they approve of, a major part of that value will be lost.

BCG estimates that two-thirds of the potential digital identity value – or about €440 billion in 2020 alone – is at risk if stakeholders fail to establish a trusted flow of personal data.

BCG estimates that two-thirds of the potential digital identity value – or about €440 billion in 2020 alone – is at risk if stakeholders fail to establish a trusted flow of personal data. All sectors face this risk, although Web 2.0 communities have the highest exposure, being strongly dependent on very sensitive digital identity applications. Nor is it digital identity value alone – the additional revenues or efficiency gains derived from personal data applications – that is at stake: Missteps in handling consumers' data can go much further, causing damage to an organisation's brand, its client relationships and its reputation.

Creating trust means that certain practices, still applied by some companies today, need to be reconsidered – practices like keeping the methods of collection and use hidden; using weak data encryption and careless employee data access schemes; offering consumers few, if any, privacy controls; and giving them a choice to "take it or leave it," which often means no choice at all. Personal data is a valuable asset for consumers and must be treated with care, in ways that inspire trust, not break it.

To unlock the full value potential, organisations need to embrace a new paradigm for digital identity applications, one that rests on three key pillars: First, they must handle personal data responsibly, ensuring an adequately high level of security. Next, they should act transparently. By being open and clear about what they are doing with private information, organisations limit the risks presented by hidden practices that, once uncovered, can become the focal point of a public firestorm. Just as importantly, transparency is critical to communicate to consumers the benefits of digital identity applications. Finally, there must be user control. As evidenced by the consumer survey commissioned for this report, individuals' preferences regarding privacy and data sharing differ – and differ widely. Options and controls allow individuals to adapt their sharing to their specific needs. While this might reduce sharing by some individuals in certain situations, overall it will likely increase the sharing of personal data.

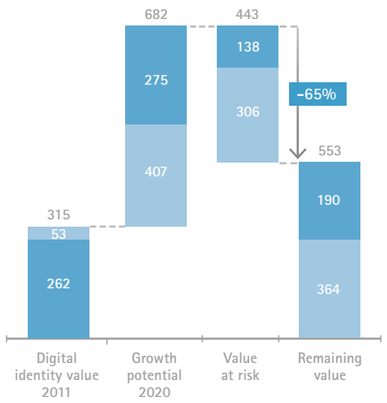
Privacy is increasingly becoming an area of competitive differentiation

By providing the right privacy controls and options, organisations can also gain a competitive advantage. Indeed, such a scenario may well play out in the desktop and mobile Web browsing market. When Microsoft announced that its next version of Internet Explorer would enable a "do not track" feature by default – so websites will know that a user does not tolerate cookies or any other tracking features – the move was clearly intended to lure customers away from competing browsers (like Firefox, Opera and Chrome) that are not expected to follow suit. Apple's Safari had already been configured to block third-party cookies by default for several years. Now, with Microsoft's initiative, two camps, each with about 50% market share, are forming in both the desktop and the mobile Web browsing market, with their approaches to privacy being key differentiators.

Another area where privacy and personal data management may likely be an important competitive dimension is the mobile operating system space. Worldwide, more than 850 million smartphones will run either Apple's iOS or Google's Android by the end of 2012.[1] Both

Digital identity value at risk

EU-27 in 2011 and 2020, billion €

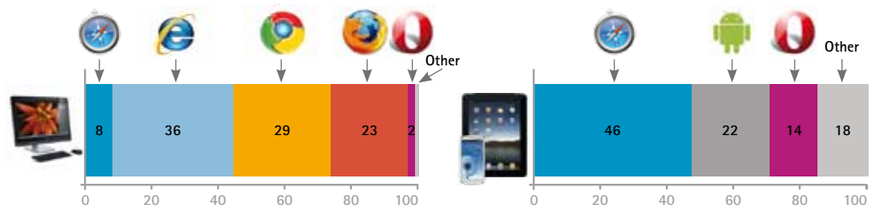


Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

Internet browser market shares

Global desktop market shares (%), July 2012

Global mobile market shares (%), July 2012



Source: NetApplications; StatCounter; W3Counter; BCG analysis

[1] Source: Gartner (July 2012); BCG analysis

platforms enable third-party apps to track highly sensitive personal data like location information. This model has already raised privacy concerns; consumers and policy makers alike are worried about data misuse by apps, particularly as the number of available apps continues to grow rapidly. Currently, neither Apple nor Google provide much in the way of user control. How they address the issue – whether they give users tools to manage their digital identities within the app ecosystem, or take no action – will have important implications in terms of both privacy and competitiveness.

Innovative approaches to building trust

However, it is not yet clear what optimal transparency and controls for consumers will ultimately look like for each digital identity application. Intense experimentation is currently being undertaken among established as well as very young organisations to find solutions that can boost consumers' trust – and their confidence in sharing their data. Below are some of the most innovative examples:

- **reputation.com.** This US-based company's mission is to help individuals and small businesses monitor their online reputations and manage how they are publicly represented on the Web. It continuously scours the Web for a client's personal data and will remove it from people-search sites. The service employs "reputation advisors" who work with users to remove or suppress any negative content about them that shows up high in Internet search results. While reputation.com's subscriber base is still limited, the company has won impressive funding from several premier venture capital funds, indicating the potential of this business model. Its most recent financing round, in July 2011, brought in $41 million, bringing total funding to $68 million.[2]

- **qiy.com**. A Dutch initiative, Qiy is a platform that aims to connect individuals with participating organisations so that the exchange of personal data is better controlled by the individual. The idea is that people should decide what information goes out, and to whom. To this end, Qiy is working to establish a trusted framework, centred around the individual, for managing access and usage rights and handling personal information. Further, Qiy intends to give users access to all of the personal data about them that is stored by the organisations taking part.

- **tos-dr.info.** Terms of Service; Didn't Read (ToS;DR) is a not-for-profit project created to enhance transparency for consumers. Terms of service and privacy policies are documents in which websites disclose how they collect and apply the personal data of their users. These documents tend not to be read. They are lengthy and often written in hard-to-understand language packed with legal terms. So individuals usually have no idea what a site actually does with their data. ToS;DR intends to change that by analysing the terms of service and privacy statement and presenting them in plain, easily comprehensible language. Each website is assigned a rating – based on its policies regarding anonymity, tracking, cookies and other privacy-related criteria – ranging from "Class A" (terms of service that treat users fairly, respect their rights and won't abuse their data) to "Class E" (terms of service that raise serious questions). One challenge ToS;DR will need to resolve is how to make its ratings widely visible to consumers, as "Class E" websites will obviously not publish their low ranking, and requiring users to research ToS;DR's own site would seriously limit its reach.

But it is not just start-ups and novel initiatives that are working on ways to boost responsibility, transparency and user control. Established companies – including some of the digital world's biggest and most influential names – are taking steps, too. Google, for example, offers users an "Ads Preferences Manager" that shows which interests behavioural targeting has derived about them – interests that are applied to deliver online advertisements that are supposed to be more relevant for the user. Through Google's tool, users not only see what interests have been stored about them, but can change them or opt out entirely.

Guiding principles to unlock the value of digital identity

Of course, the challenge now is for organisations to adopt the new paradigm. To help guide them on their way, we have developed the following principles:

- **Engage customers for sustainable personal data usage.** Organisations should involve and educate consumers on personal data applications, as well as on privacy management. And they should do so in a carefully thought-out, well-structured way. As we show in this report, three elements are essential to ensure a sustainable flow of data: First, the benefit a consumer receives has to exceed the "cost" of sharing the data. Second, there needs to be transparency on how the data is used. Third, privacy controls should be available and easy to use. Dialogue and interaction with consumers – in an ongoing process – is critical to getting these elements right.

- **Take accountability for a trusted flow of data.** Every business and public agency that depends on digital identity applications should define guiding principles for how it works with personal data. These principles should be communicated clearly both within and outside the organisation to ensure unmistakable accountability and commitment. At the same time, an organisational structure and processes that hardwire compliance with those principles should be established.

- **Increase data security in order to safeguard digital identity.** As the examples in this report demonstrate, data breaches cause damage on multiple fronts: Consumers see their personal information compromised; organisations see trust erode and their brand and reputation suffer. There are the direct costs, as well, to both the consumer and the organisation. The level of security – not just technical measures, but also policies and access control – must reflect the high value of personal data.

- **Build a data-driven organisation, not just a data-driven IT department.** Consumers aren't the only ones who benefit from transparency. Organisations do, too. They should know what data is available both inside and outside their

[1] Source: http://www.crunchbase.com/company/reputation-com

A PRACTITIONER'S GUIDE

own walls, and all parts of the organisation should be encouraged to identify value creation opportunities, experiment with new applications and develop analytical talent.

While safeguards are needed, the regulations that ultimately result should be flexible enough that consumers can make their own informed choices about whether and how they share data.

Striking the right balance in policy and regulation

Across Europe, policy makers are actively discussing proposed rules on privacy. While safeguards are needed, the regulations that ultimately result should be flexible enough that consumers can make their own informed choices about whether and how they share data. Individuals should be able to generate value from their digital identity – if they wish to do so. At the same time, they should be able to rest assured that their data isn't being put to unintended or undesired purposes.

Once again, balance is key. Privacy protections shouldn't be so stringent that they discourage innovation, nor should they be so weak that they enable misuse. It also requires sometimes taking a step back from some of the emotion that can imbue discussions on privacy. Politicised and hyped concerns about the privacy implications of new applications – concerns voiced recently in the case of Google's "Street View" feature – can morph into widespread outcry as it did in Germany. That, in turn, could trigger blanket prohibitions on certain data uses – which might impact a wide range of applications beyond the targeted one. Ultimately, while well intended and designed to protect individuals, such prohibitions can actually hamper or delay innovations that would benefit them – and would put domestic industries at a competitive disadvantage relative to their international competition. Balance also means that sometimes a "highest" level of protection that stalls novel new applications is less desirable than a "high" level that spurs them.

The most successful policies will put the consumer front and centre, but also enable experimentation in, and development of, new uses of personal data. They will be firm regarding principles, but will allow for flexibility in implementation and enforcement. They will give organisations a certain amount of leeway, acknowledging that different markets and regions have different historical, cultural and political legacies – and different, constantly shifting attitudes towards privacy and new uses of personal data.

A balanced approach, both in policy and in the applications themselves, is essential to realise the full potential digital identity has to offer. This challenge is not limited to Web 2.0 communities or the digital economy, but is highly relevant for the economy as a whole. Putting the consumer at the centre of the discussion is the right way to address digital identity. The guiding principles for capturing the benefits of personal data applications should be based on how individuals view their digital identity and what influences their decision making. There is a lot at stake here. Digital identity isn't just about data and opportunities and growth. It will impact our lives and our society. It will change the way we interact with the world around us. It will shape our future.

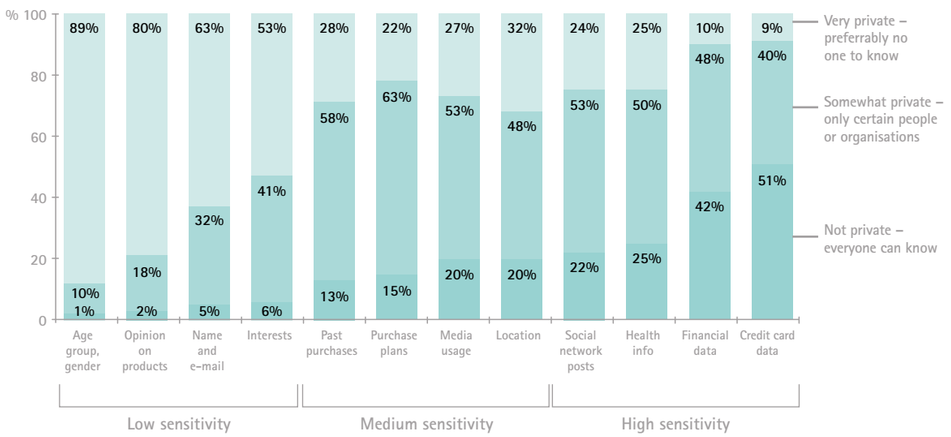
appendix

APPENDIX

The four exhibits on the following pages present additional results of the consumer research referred to in part 2 of this report, conducted exclusively for this study.

Assessment of privacy level per data type

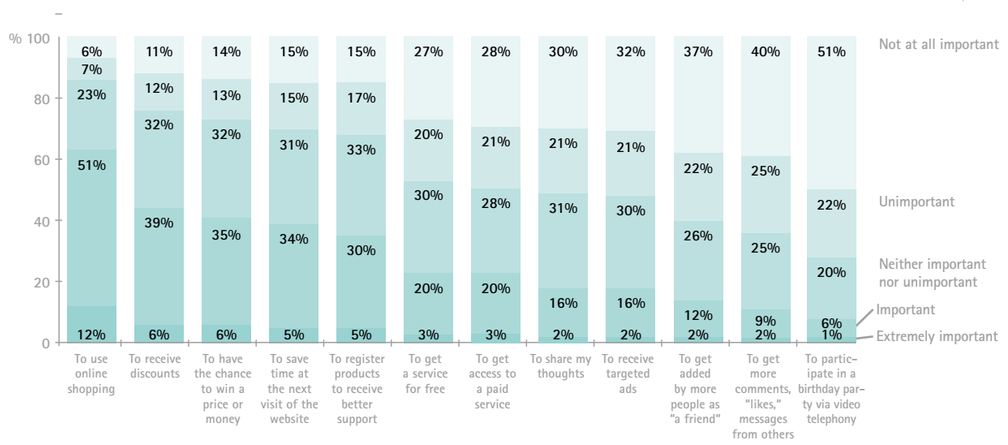
How private do you consider the following data types?



Note: Numbers may not sum to total due to rounding.
Source: BCG digital identity survey (n = 3,107, August 2012)

Importance of reasons to disclose private data

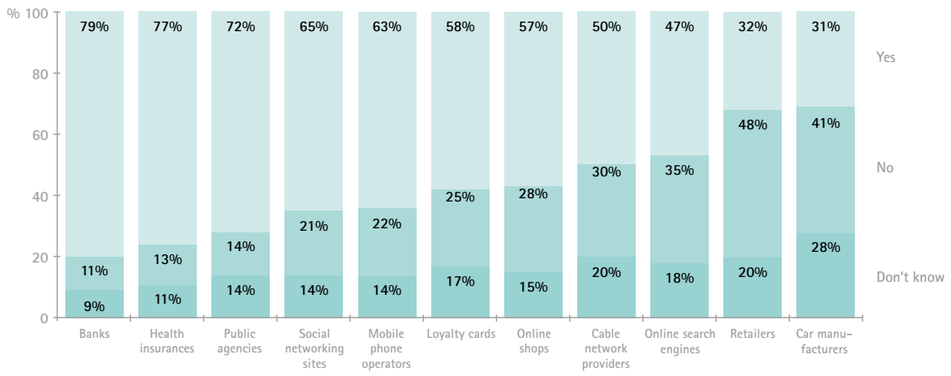
How important are the following reasons for you to disclose your private data?



Note: Numbers may not sum to total due to rounding.
Source: BCG digital identity survey (n = 3,107, August 2012)

Awareness of data collection by sector

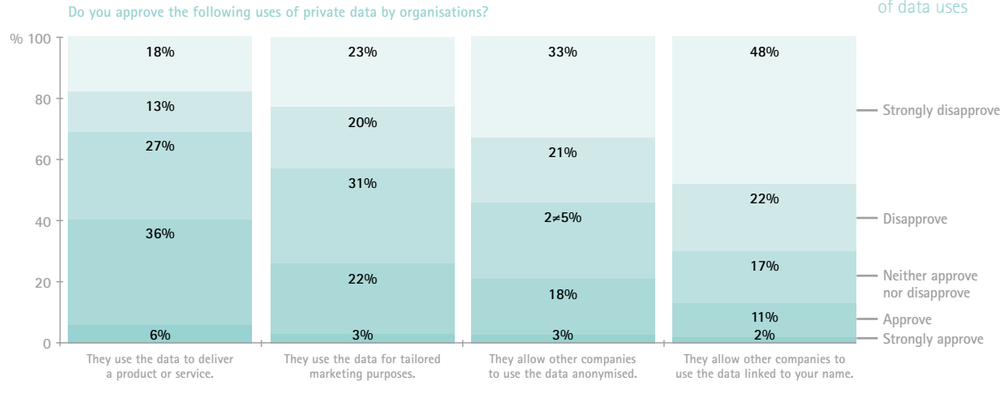
Are you aware of any of the following organisations collecting data you consider "very private" or "somewhat private"?



Note: Numbers may not sum to total due to rounding.
Source: BCG digital identity survey (n = 3,107, August 2012)

Individuals' approval of data uses

Do you approve the following uses of private data by organisations?



Note: Numbers may not sum to total due to rounding.
Source: BCG digital identity survey (n = 3,107, August 2012)

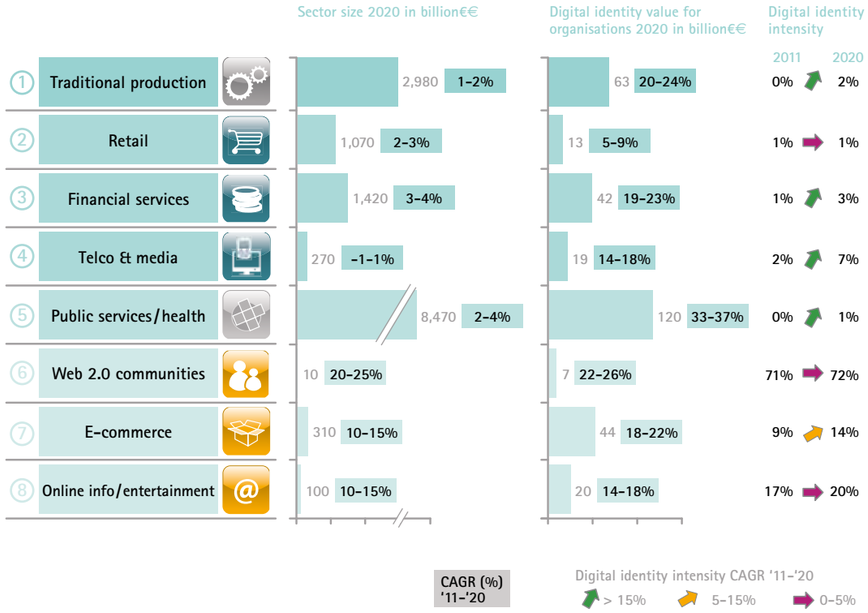
APPENDIX

The exhibit below provides an overview of how we assigned the „digital identity value share" – the estimated share of digital identity value of an application's overall value generation – for each use case to reflect the particular importance of personal data to that application. The exhibits on the following pages depict the resulting digital identity intensity by sector and show how we defined the sector size for the purposes of this study.

Application of digital identity value shares in quantification model

Digital identity value share	Assessment per digital identity value share
Very low = 20%	Digital identity is minor value contributor and majority of value add is provided by other elements *Example: Digital identity only used for secure authentication and payment in e-commerce, but major value represented by purchased goods*
Low = 40%	Personal data contributes value to product/service, though other elements responsible for most value contribution *Example: Binding customers with rewards is major goal of loyalty programmes, but insight generated from personal data for demand planning and optimisation*
Medium = 60%	Personal data is important value contributor and product/service can not be delivered without it, other elements remain important *Example: Personalised medicine not possible without personal health data; but IT capabilities, R&D and medical treatment also important within process*
High = 80%	Personal data is key enabler for value generation and delivers most value of service/product *Example: In social networks, personal data is the product and key for monetisation via advertisements through third-party applications, other apps such as games contribute small share of value*
Very high = 95%	Personal data represents (almost) entire value of product/service, remainder of value retrieved from minor supportive activities *Example: Companies selling contact details of consumers in various demographic and behavioural segmentations based on acquired permissions*

Development of digital identity intensity per sector



Note: Digital Identity intensity = estimated share of digital identity value of overall sector size
Source: Company reports; EITO; EIU; Gartner; Eurostat; OECD; IDC; Forrester; IAB; BCG economic value modelling

APPENDIX

Sector size definition to assure comparability of digital identity intensity across sectors

	Sector size 2011 in billion €	CAGR '11–'20	Sector size definition	Sources
① Traditional production	2,700	1–2%	Total sector revenues minus retail gross margin[1]	Euromonitor International, EIU
② Retail	850	2–3%	Retail gross margin[1]	Euromonitor, "Einzelhandel"
③ Financial services	1,050	3–4%	Revenues of retail banking, asset management and insurances	BCG analysis, Cerulli Associates, SwissRe
④ Telco & media	280	-1–1%	Total sector revenues	EITO Industry Report
⑤ Public services/health	6,630	2–4%	Total government[2] and health care expenditures	Eurostat
⑥ Web 2.0 communities	1	20–25%	Total sector revenues	BCG analysis
⑦ E-commerce	100	10–15%	Total sector revenues	Forrester research 2011, Eurostat
⑧ Online info/entertainment	30	10–15%	Total sector revenues	BCG analysis

Note: Digital Identity intensity = estimated share of digital identity value of overall sector size

[1] In order to make retail sector size comparable, only the retail gross margin is considered to account for the high share of purchasing costs; this margin is then deducted from traditional production (sector from which retail purchases goods) to avoid double counting

[2] Including intermediate consumption; employee compensation, subsidies, consolidated property income, other consolidated current transfers, social benefits, consolidated capital transfers, gross capital formation

Liberty Global commissioned The Boston Consulting Group to author a study on the topic of digital identity in the context of the European economy. The objective of this work is to contribute to a debate currently high on the agenda of industry, policy and regulation with a quantitative angle on the value of personal data applications, empirical evidence on consumers' actual data-sharing decision making and a holistic perspective. The study reflects BCG's thoughts on the topic of digital identity, supported by industry analyses as well as case studies and company examples based on publicly available information. In the process of writing the study, over 15 European industry managers and policy makers were interviewed whose expert contribution is reflected in this work. The study provides a basis for discussion for key stakeholders across public and private sectors on a broad set of topics related to digital identity developments and future strategic, policy and regulatory priorities.

For further information or additional perspectives, please contact:

John Rose
Senior Partner & Managing Director
BCG New York
rose.john@bcg.com

Olaf Rehse
Partner & Managing Director
BCG Düsseldorf
rehse.olaf@bcg.com

Björn Röber
Project Leader
BCG Düsseldorf
roeber.bjoern@bcg.com

November 2012