Digital identity's role in optimizing customer experience and competitive advantage

KPMG International

kpmg.com

Consumer identity has a new face in the digital age

Creating the ultimate customer experience is climbing higher on the agenda of businesses embracing digital transformation to meet today's — and tomorrow's — customer expectations for personalized service that's accessible anywhere, anytime.

As businesses become increasingly customer-centric, many are also discovering the importance of *consumer identity* as a significant customer-experience differentiator.

Digital consumer identity is evolving from a security-focused capability to become a key element of customer-engagement strategies aimed at attracting and retaining customers and delivering new levels of value and growth. Simply put, organizations that are elevating their approach to digital or consumer identity beyond security compliance are transforming the way they deliver value to their customers and businesses.

Digital identity's central role in forging the personalized customer experience — bringing together ease-of-use and accessibility with security, privacy and control of consumer data — should be a key component of any organization's digital transformation agenda today.

Organizations can position themselves to deliver new products and services with enhanced speed, agility and competitiveness — supporting consumer choices on privacy while optimizing security via authentication and authorization methods such as biometrics based on physical attributes, behavioral attributes or imaging (face or iris recognition).

Conversely, organizations ignoring the advantages of digital identity capabilities can expect to fall a step or two behind in the race to provide services and experiences that customers have come to expect, ultimately failing to foster brand loyalty and long-standing relationships.

"Businesses failing to fully integrate *digital identity* with wider customer engagement strategies risk fragmented, disjointed customer experiences and customer attrition, not to mention the inability to capitalize on customer data, predictive analytics and insights that will ultimately inform decision-making and enhance the overall customer experience," says Jan Zeilinga, Chief Technology Officer, Cyber Security Services, KPMG Australia. "Worse, a lack of holistic thinking around digital identity may fail to protect customer privacy choices and confidential data. Companies with poor digital identity capabilities risk displacement by more-agile competitors"

A recent study by Oxford Economics and the CGI Group found that a significant breach of public companies results in a nearly 2 percent permanent loss in value.[1]

From 'policing' access to enabling it, digital identity assumes a new role

The role of digital identity as a business enabler represents a major departure from the past. Until recently, it was synonymous with cyber security technology and the concept of identity and access management (IAM), with its focus on enterprise and workforce security and operations.

With the digital transformation of business models and the intense focus on customer-centric strategies, digital identity has evolved into the broader field of *consumer identity and access management* (CIAM).

Organizations traditionally have invested in *enterprise identity and access management* (EIAM) for security functions such as access governance and cyber-risk mitigation. Simply put, EIAM systems have typically served more of a 'policing' role in strictly controlling access to enterprise systems. CIAM systems play more of a 'concierge' role — directing and overseeing access to today's digital products and services. In this way, consumer identity also plays a role in differentiating the customer experience and making businesses more competitive. The quality of the 'concierge' experience can be the difference between delighted customers enjoying loyal brand relationships, and frustrated customers who turn to the competition.

Organizational response to digital identity

CIAM and EIAM both rely on digital identity concepts, solutions and capabilities but have different stakeholder groups within organizations, plus diverse applications.

CIAM is generally the domain of decision-makers focused on business opportunity and growth, including the chief digital or data officer (CDO), chief marketing officer (CMO), chief information officer (CIO), heads of business units and the CEO. These leaders and their teams are building consumer identity systems designed to identify customer preferences and to respond with relevant, timely, highly personalized experiences.

EIAM, however, is the domain of decision-makers focused on risk and operations — including the chief risk officer or head of regulatory compliance, CISO or CIO. These stakeholders have their sights set on compliance, risk, governance, security, privacy, employee lifecycle management and operational efficiency.

Given their diverse functions and requirements today, deploying different systems to manage CIAM and EIAM is common. KPMG member firms have extensive delivery experience and success working in both domains and has invested in governance models, technology platforms and the ability to execute across both stakeholder groups. Our experts are delivering timely insights and perspectives aimed at optimizing these critical dimensions of identity for success in the digital age.

[1] Serious Breaches Shave Nearly 2% Off Public Company's Value by Mara Lemos Stein, April 2017 http://bit.ly/2nJpSFi

New digital identity strategies are driving competitive advantage

Organizations aligning their approach to digital identity across both CIAM and EIAM domains are driving significant new levels of business value. Firms undertaking digital transformation and omnichannel customer engagement strategies today can easily encounter capability and technology gaps when it comes to managing consumer identity.

Taking a holistic, enterprise-wide approach to consumer identity maximizes the value of investments while dramatically heightening security, agility and responsiveness to the marketplace. It's no surprise, then, that digital consumer identity is climbing up the business agenda and driving more board-level discussions.

This new strategic focus is creating opportunities to exploit the benefits of consumer identity at various levels, while overcoming traditional reliance on a siloed departmental approach that risks ongoing inefficiencies, duplication of effort, higher costs and limited agility.

Executives planning CIAM investments should consider their role as *change agents* in delivering:

— Personal and meaningful customer engagement;

— Authentication innovation;

— Secured, private customer data and respect for customer preferences on data use;

— Participation in digital ecosystems;

— Regulatory compliance.

Personal and meaningful customer engagement

Omnichannel customer engagement

The proliferation of digital customer relationships and the resulting rise in consumer expectations for personalized service and choice are now a board priority at many organizations, prompting many to appoint a chief digital officer to take responsibility.

Today's increasingly connected, mobile and sophisticated consumers and business clients in any industry are demanding consistent personalized experiences across every traditional and digital channel, whether the interaction is in-store, via telephone, online, smartphone-based or employing automation and artificial intelligence (AI).

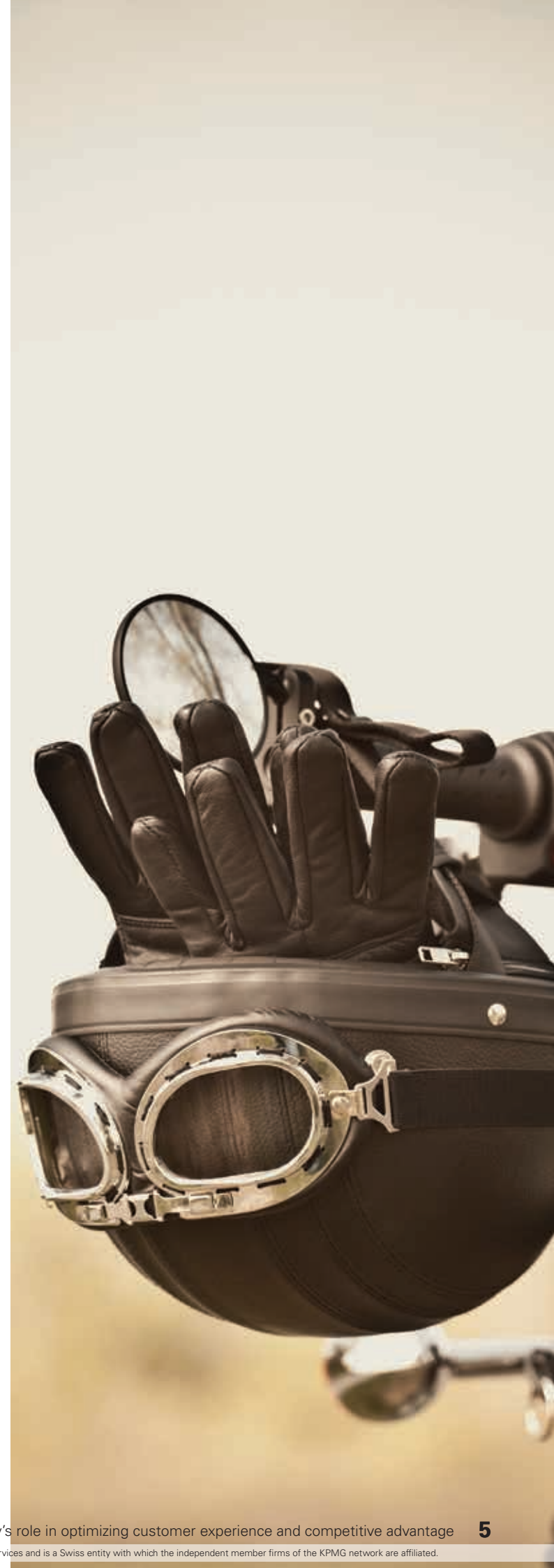
Omnichannel engagement is thus challenging organizations possessing diverse systems to service both their operational and digital identity environments.

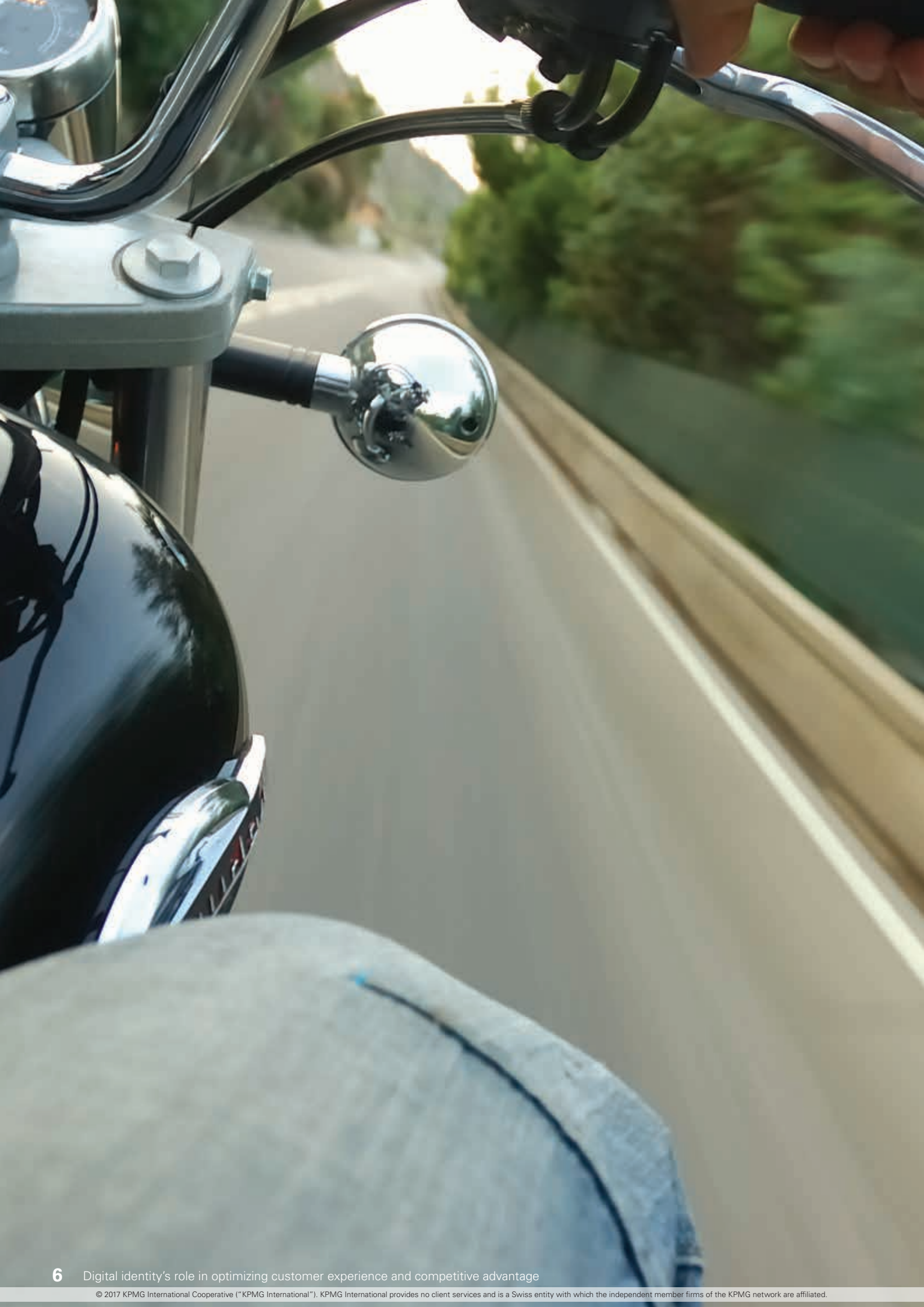
CIAM systems consolidate and link, within a single system, digital identity data that's typically scattered across multiple enterprise systems and databases. They create a data-rich platform that can help to significantly deepen customer relationships by delivering new levels of customer familiarity and service. A consolidated view of customers also has compliance benefits, ensuring customers are addressed with correct entitlements based on purchase history, for example.

Customer engagement and exchanging value

Creating meaningful, valued customer experiences requires more than creating a single view of customer data, however. Continually engaging customers, via ongoing digital and social media conversations, is also instrumental in the endless quest to build loyal relationships and brand value. The array of customer data that's available today underpins and drives these digital conversations — whether transactional data, relationship data or analytical insights that help to interpret interactions and preferences and anticipate future needs.

Consumers certainly value the familiarity they can develop over time with, say, a local retailer or service provider, and may feel disappointed when a familiar face leaves. We value relationships involving someone who understands our preferences and can provide better service. Fortunately, today, digital channels are delivering customer data that can be used to forge unprecedented levels of customer familiarity and service, generating deeper insights into behaviors, preferences, motives and desires. Increasingly, marketers are aiming to create the 'internet of me' experience for customers, using online interactions across news, social, search and commerce channels to precisely tailor each individual experience.





Consumers often entrust identity data to organizations with an expectation that it will be securely used to generate relevant and appropriate interactions. For example, your social media profile might reveal your interest in cultural activities such as music festivals, and a company could use that information to target timely offers and discounts. Location can also be used to trigger relevant and timely communications that delivers value and deepens customer relationships. A customer traveling to a holiday destination might gladly receive local traffic or weather alerts, event recommendations and tourist information via appropriate channels.

BYOID and 'conversational commerce'

Many consumer identity solutions enable customer ID via social media and search platforms and other services. This 'bring your own identity' (BYOID) offers new levels of speed and convenience during customer interactions. The scale of consumer identity platforms — often orders of magnitude greater than traditional Enterprise IAM solutions — drives organizations to consider more convenient methods of registration and sign-on such as, use of third party social identities.

With the advance of AI and cognitive capabilities, we are starting to see the conventional user interface disappear in favor of natural language-based dialogue known as *conversational commerce*. More than 10 million businesses in China, meanwhile, use WeChat for transactional capabilities that promise significant revenue growth by allowing consumers do it all, whether paying a water bill, ordering customized Nikes, shopping at Burberry or ordering lunch via a chat interface.

As these services and others proliferate, a digital identity that's secure and trusted across a number of partner organizations or third parties will be essential.

Authentication innovations heighten convenience

Digital technology has placed a dazzling array of choices into the hands of mobile customers via their smartphones, along with innovative new authentication and authorization methods. Examples include new facial recognition systems and the emergence of behavior biometrics for continuous authentication.

As this trend continues, there are good reasons for organizations to embrace new authentication methods that offer instant and reliable access:

— **Security.** The risks associated with usernames and passwords are well understood, but every authentication method has a certain risk profile. If compromised, they need to be replaced quickly and painlessly to minimize disruption. In addition, emerging governmental and regulatory standards such as the National Institute of Science and Technology (NIST) draft publication 800-63-3 are driving replacement of traditional user name and password methods with new and improved solutions.

— **Convenience.** Organizations can already authenticate customers via voiceprint: Instead of a username/password entry, customers simply say 'Hello' for instant access and a level of uber-convenience that's sure to create new competitive advantages for firms.

— **Customer expectations.** If you are the only organization in your sector that doesn't support BYOID, or two-factor authentication for high-value transactions, customers will soon perceive your services as less convenient and secure — a powerful incentive to choose a more innovative competitor.

Forward-looking businesses are thus increasingly responding with resources and investments that will deliver state-of-the-art authentication methods to meet consumer expectations.

An *identity services framework*, one supporting 'pluggable' authentication and authorization services, can quickly and efficiently provide the required agility to deliver during every interaction with customers. When someone logs in from a new device for the first time, for example, they may need to answer a secret question. These easy interactions boost security and build trust with customers.

Delivering popular new customer services while managing today's pervasive cyber security threats are crucial capabilities for every identity services framework. This includes algorithms that both detect suspicious access attempts and instantly step up authentication with additional security factors such as fingerprinting of mobile phones or tablets. While banks need risk-based algorithms for fraud detection, for example, they can also simplify authentication for customers. Rather than rejecting a suspicious access request, systems can seamlessly step up the level of authentication required and minimize disruption to genuine customers.

Secured private customer data and respect for customer preferences

The proliferation of data today is immensely useful but careful data management is critical. Data and analytics processes can be misused or abused. As an example, organizations can alienate customers with offers based on data that customers consider private, outdated or simply inappropriate.

Data and analytics platforms raise the risk of privacy invasion — particularly when using social media or geospatial data — if explicit consent is not clearly requested and granted. Some customers may be comfortable sharing location data or info about lifestyle or work, while others will not. For example, not all customers will wear a fitness device and commit to an exercise regime just to save money on health insurance; others will decline offers to install a sensor in their vehicle to monitor and report on driving habits that will impact insurance premiums.

At the same time, the exchange of privacy for security can be seen as a good trade-off. The recent KPMG survey report *Crossing the line: Staying on the right side of consumer privacy*, found that 78 percent of consumers surveyed globally liked the idea of vehicle location-tracking designed to help emergency services locate them when necessary.

With consumer identity systems, data analytics can be paired with customer engagement processes to manage customer preferences at all times. Increasingly precise preference- and permission-management capabilities offer organizations a significant competitive edge via data and analytics — when used wisely.

Participation in digital ecosystems

Value creation through a digital ecosystem

Secure *application programming interfaces* (APIs) have emerged as a mechanism to open up corporate information silos and business functionality. APIs enable a new business model that shares data with external developers, mobile devices, digital ecosystems and other cloud-based services through a commoditized interface.

APIs rely on digital identity to authenticate all participants in an information exchange and prevent data leakage, and can be implemented within an identity services framework. Affiliates or partners may also rely on an organization's consumer identity systems to understand the source of data, how it will be used and whether there is appropriate consent.

Getting ready for the Internet of Things

The Internet of Things (IoT) is an exploding network of connected objects designed to collect and exchange data using embedded sensors that are already creating smart homes, workplaces and cities, along with connected vehicles, transportation systems and much more. Estimates vary but experts anticipate between 20 and 30 billion connected devices to be operating by 2020.

This phenomenon is already ushering in a wave of disruptive new threats as well as opportunities. One of the biggest IoT issues involve managing the ongoing process of securing connected devices and the information they will collect and expose across multiple connection points, many of which are vulnerable to cyber attacks. There is enormous potential here for organizations to fail in their efforts to meet expectations regarding customer privacy and security.

This is particularly true as digital services to which IoT devices are connected involve third and fourth parties and outside ecosystems: organizations will increasingly be functioning within several supplier ecosystems, not all under their direct control regarding IoT device access and security.

A typical consumer device like a digital fitness monitor already operates within a complex ecosystem. Digital identity needs to control not only the device but the services it's connected to and the information it shares, at all times on customer preferences and authorization.

These ecosystems will be secure and useful only as long as customers retain control of their digital identity, the primary access and control mechanism within IoT ecosystems. Organizations will need to evolve their identity services and security measures to meet both customer preferences and privacy/security expectations. Firms responding quickly today can drive new competitive advantages.

Regulatory compliance

As organizations employ sophisticated data analytics and cognitive computing to understand the behavior of customers and clients, the risk and cost of data breaches increases, particularly as more data is shared among affiliate or partner organizations and across global digital ecosystems.

As a consequence, privacy regulations are on the increase. The European Union's General Data Protection Regulation (GDPR), which comes into full force on May 25, 2018 after a two-year transition, extends current EU data protection rules to cover the data of any EU resident held by foreign companies. With non-compliance penalties of up to 4 percent of global revenues, boards of many non-EU companies are paying close attention.

Not surprisingly, perhaps, boards are addressing both their regulatory and reputational concerns by asking more questions of their marketing or the digital business units about privacy and the security of personally identifiable information (PII). And while many boards are confirming that current consumer identity initiatives or systems are in place, they are also learning that without appropriate corporate oversight and strategies, there is no guarantee of proper privacy and cyber-security protections.

Consider one high-profile example, involving a popular global retailer's mobile wallet and payment app that, unfortunately, stored user names, passwords, email addresses and geolocation data as clear text on each customer's mobile device, putting their confidential data and financial accounts at risk.

Compliance with evolving regulations, and the need for increased cyber security as the technology environment and consumer marketplace continue to evolve rapidly, should be viewed by organizations as a key *business issue* — not simply an IT issue for the tech team to solve amid the proliferation of new technology, capabilities, authentication services and risk levels.

Organizations need to take an enterprise-wide approach to these fast-emerging trends, rather than relying on the traditional 'siloed' or departmental approach that limits efficiency, security and agility in the digital age.

Conclusion: An enterprise response to digital identity

By taking a holistic, 360-degree, 'single enterprise' approach to consumer identity, organizations can quickly and efficiently implement critical new security foundations that mitigate risk while delivering choice, convenience and reliability across every customer touch point. The following guidelines are key areas to consider:

— **Change management starts at the top.** Senior management and boards are becoming aware of significant risks, costs and missed opportunities in a siloed approach to consumer identity. Discussions about digital identity are moving up from the CDO, CMO or directors of infrastructure or business applications to CEO or the board level. Senior executives need to see themselves as proactive *change agents* in today's digital business environment.

— **Sharpen your view via identity services frameworks.** Leading organizations are taking a 'single enterprise' approach to digital identity. An identity services framework enables new customer-centric functions and adoption of emerging trends, by tethering digital identity to channels, devices, risk, user experiences, consent, preferences and privacy needs.

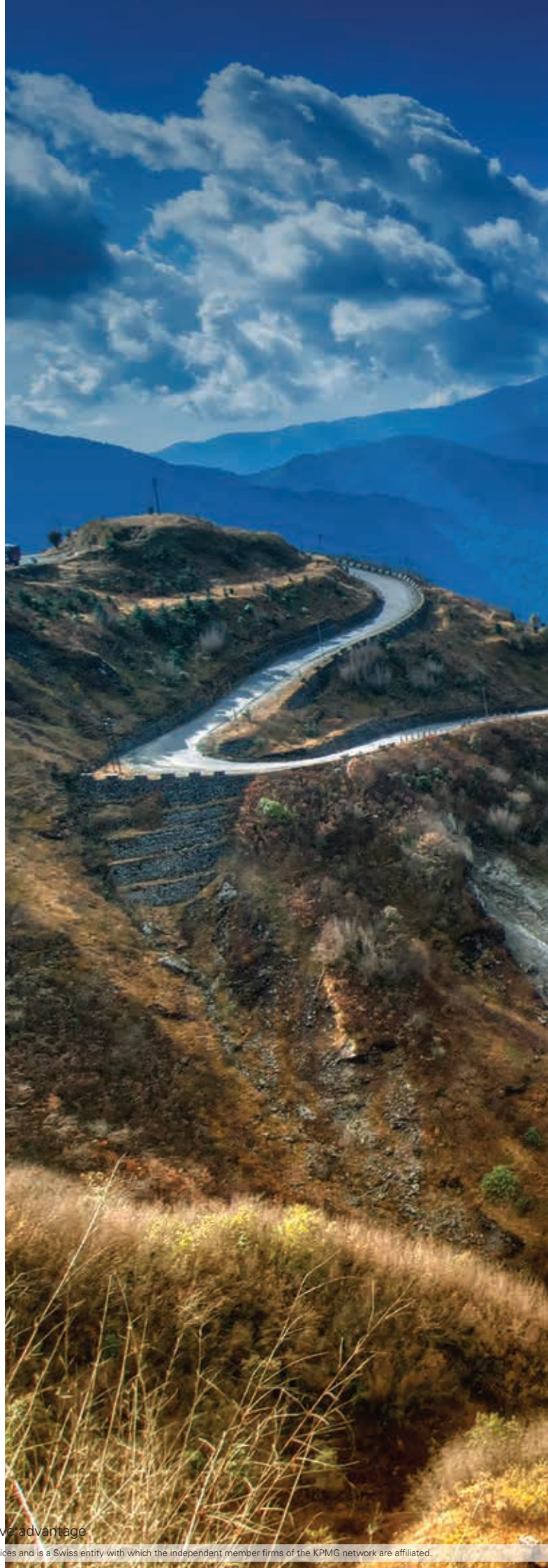
— **Governance of the entire ecosystem as it expands.** Consumer identity initiatives benefit from similar governance and access controls to enterprise identity and access management systems. Many data leakages come through affiliates or partners. Mitigating those risks requires strong governance of digital ecosystems, plus clear ongoing communication with clients through customer-facing digital platforms.

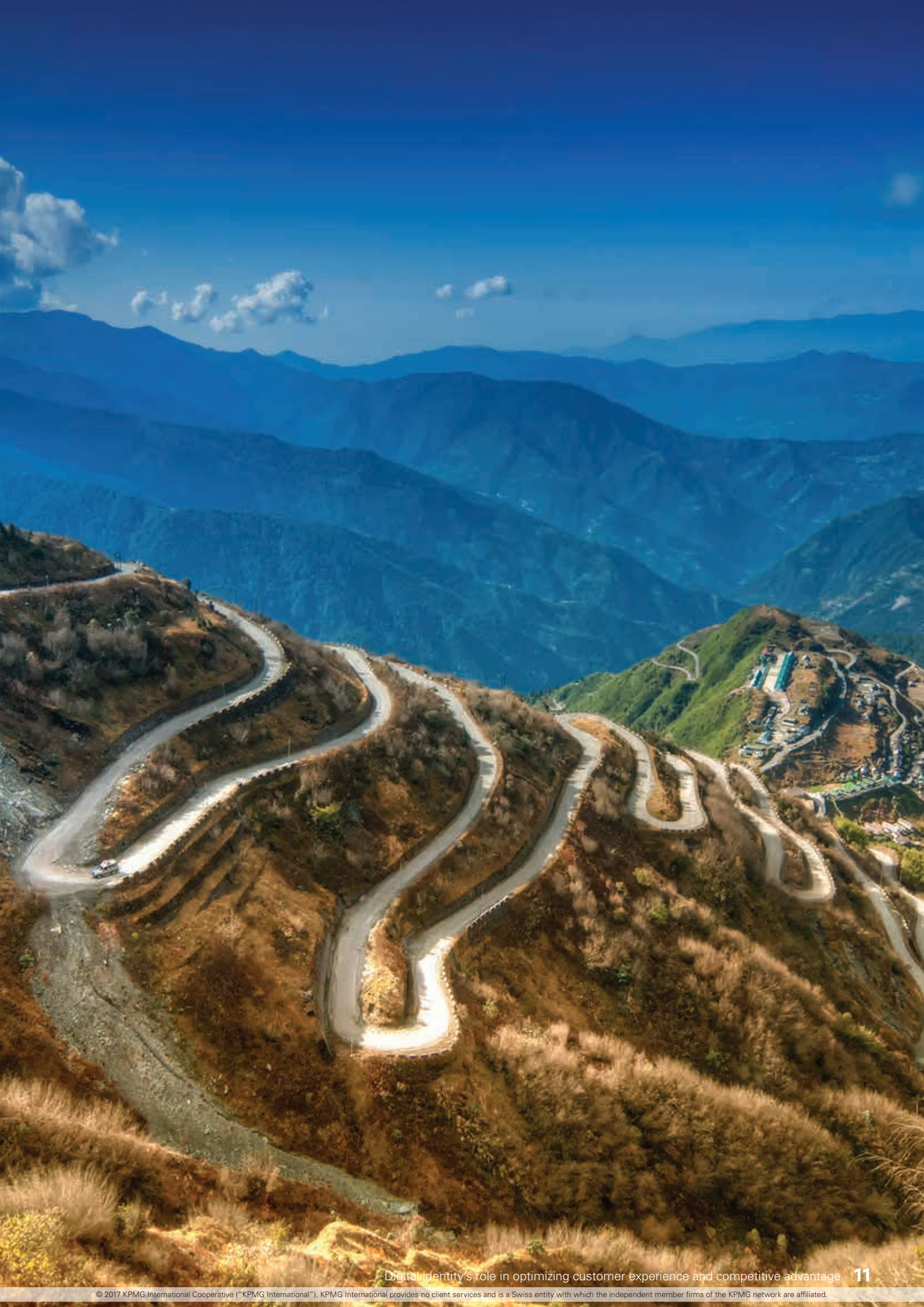
— **Preferences are personal.** Organizations cannot take a one-size-fits-all approach. There are significant differences between how CIAM systems and EIAM systems communicate with their users. Different customers or clients have different expectations of privacy and security, making two-way dialogue that takes customer preferences into account vital to the CIAM success.

— **Know and respect privacy concerns.** Consumers want to understand and control where and how personal information is used. Different customers will make different choices based on their own risk/reward profiles. Organizations that respect their wishes and gain a reputation for protecting privacy will gain a competitive advantage over those that don't.

Here's how KPMG firms can help.

KPMG's Cyber Security practice works alongside clients to implement identity services based on consumer identity technologies. These manage the lifecycle of identities and their relationships, and provide a data exchange ecosystem and a set of business processes to simplify realization and enable agility. Potential benefits include reduced risk, cost and time to value, and an improved customer experience that helps organizations attract and retain customers and build new business.





Authors:

Jan Zeilinga
Chief Technology Officer
Cyber Security Services
KPMG Australia
E: jzeilinga@kpmg.com.au

Santosh Haranath
Specialist Director,
Cyber Security Services
KPMG in the US
E: santoshh@kpmg.com

Tracy Moore
Director,
Solution 49x
KPMG Australia
E: tracymoore@kpmg.com.au

Jacob Pszonowsky
Managing Director,
Cyber Security Services
KPMG in the US
E: jacobpszonowsky@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia

Designed by Evalueserve.
Publication name: Digital identity's role in optimizing customer experience and competitive advantage
Publication number: 134497B-G
Publication date: August 2017