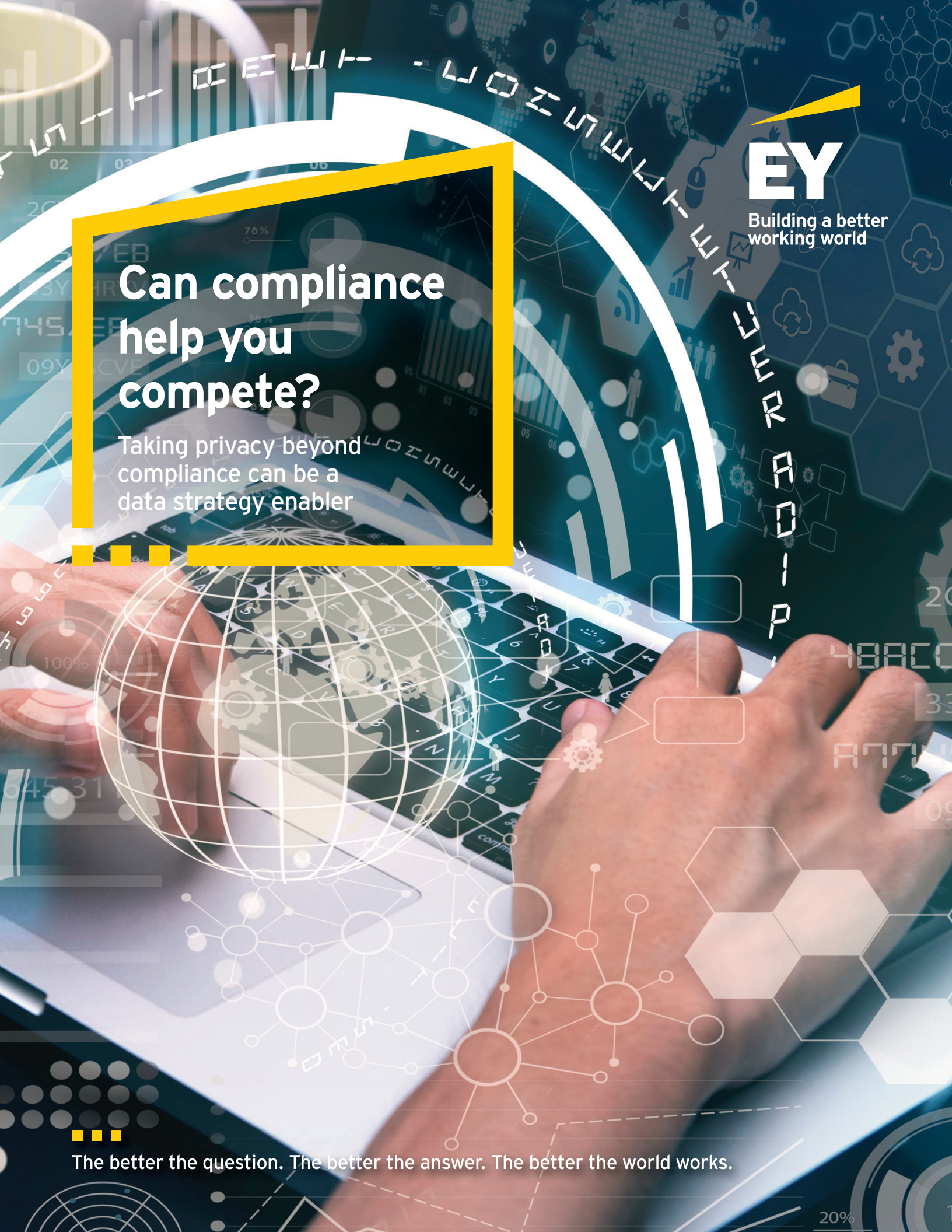


Can compliance help you compete?

Taking privacy beyond compliance can be a data strategy enabler

EY
Building a better working world

The better the question. The better the answer. The better the world works.

Privacy is not only a compliance issue. It's strategic!

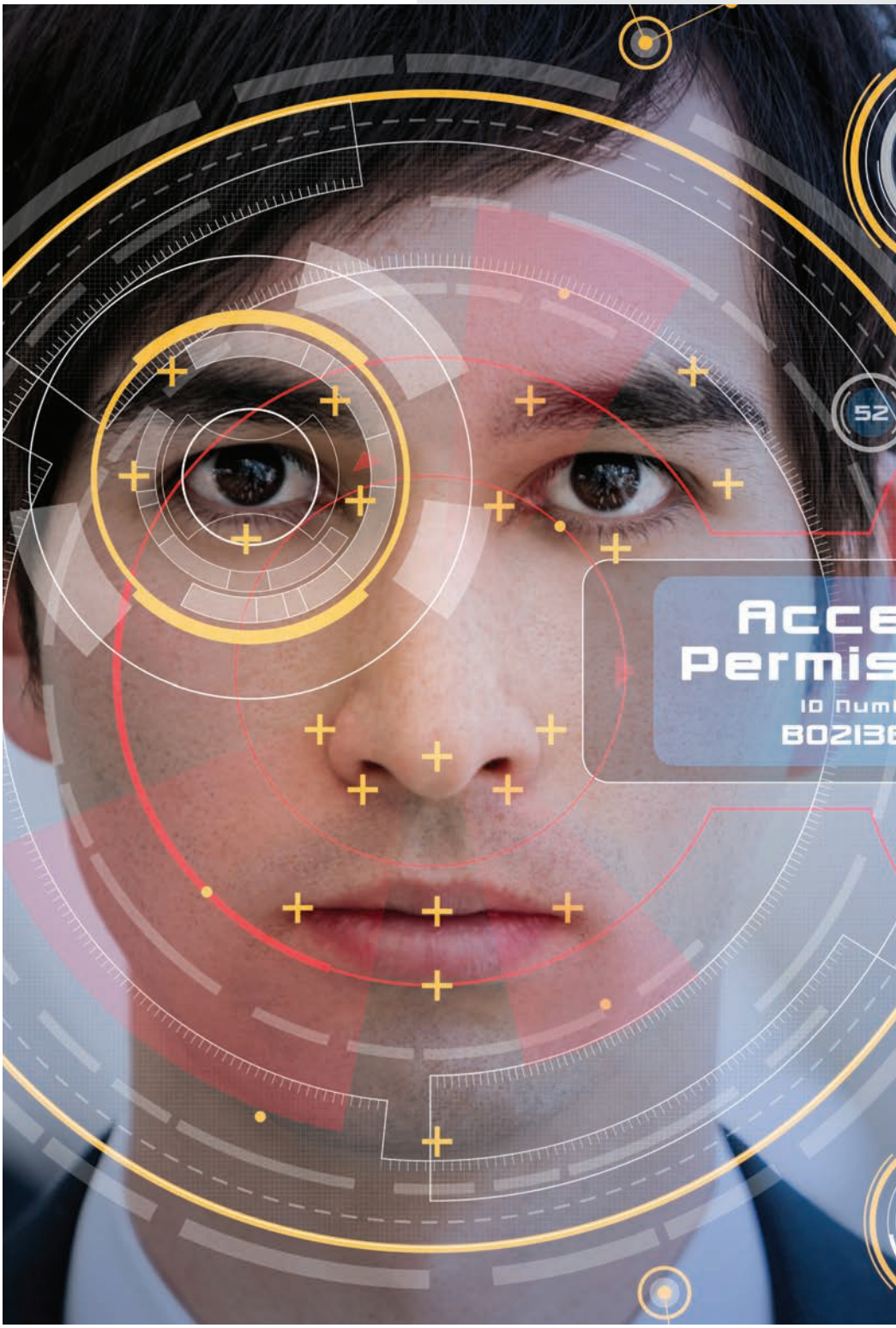
Leading organizations are placing greater strategic importance on advanced analytics, and they're investing in the people and resources to embed it more deeply into business decision-making.

A recent survey conducted by EY and Forbes concluded that the drive and need to capitalize on advanced analytics is being fueled by fundamental changes resulting from new digital technology. Among the most impactful to the global enterprises surveyed are the rise of the Internet of Things, increased concerns and regulation surrounding data privacy and security, and the shift of IT resources to the cloud.[1]

While big data promises significant economic and social benefits, it also raises serious privacy concerns. In particular, big data challenges the Fair Information Practices (FIPs), which form the basis of all modern privacy law. Probably the most influential privacy law in the world today is the General Data Protection Regulation (GDPR). But while the GDPR addresses issues related to targeting, profiling and consumer mistrust, it relies heavily on a discredited informed choice model, and therefore fails to fully engage with the impending big data tsunami.

With the vast amount of personal data that's in cyberspace, consumers are becoming more aware of what information is out there about them. As a result, organizations need to step up and be more transparent about consumers' online lives, provide options for them to own their data and restrict the use of their data, and obtain explicit consent for each purpose for which their data will be used.

Organizations often ask to collect and retain some personal information because it provides a better user experience.



[1] *High stakes, high rewards: data & advanced analytics in Canada*, Forbes Insights, EY Canada, 2016.

That may be true, but the price consumers are paying is invaluable data that can make organizations money. It's irresponsible for organizations to ask consumers for their consent in this way, and it can lead to data breach fines, reputational damage and of course a decreased level of consumer trust.

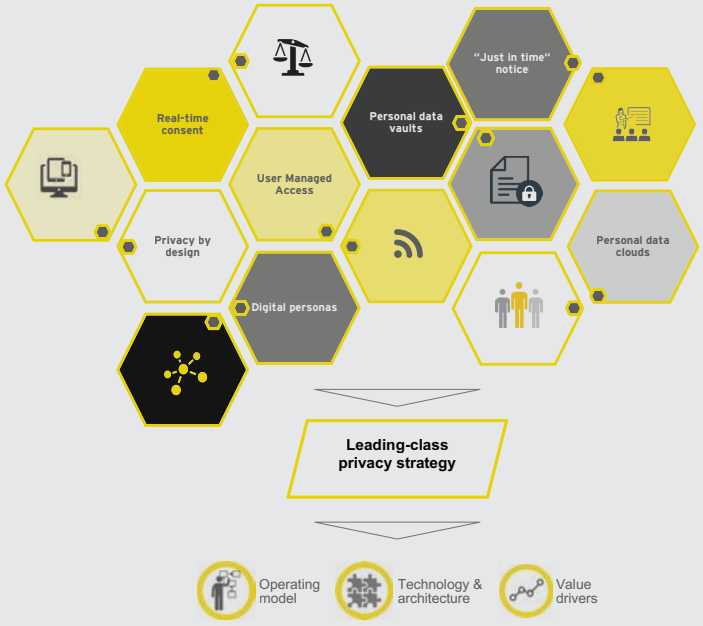
Organizations that want to reap the significant economic and social benefits advanced analytics can bring need to create a data privacy strategy that goes beyond compliance. The strategy must combine legal reform with the encouragement of new business models that are premised on consumer empowerment and supported by a personal data ecosystem.

This new strategy is important because it changes the focus of who benefits from the collection and use of personal data from businesses to consumers. It also increases consumers' trust by giving them control over how their data is collected and used while still benefiting from the use of big data.[2]

Overall, enabling individuals to take control over their identity and managing the ethical implications of data use will become a market differentiator for organizations. While some may choose minimum compliance to legislation like the GDPR, forward-thinking organizations will shift their data strategy to enable methods of harnessing customer intention as opposed to simply reacting to customer behaviour.

So how can organizations shift their data strategy from creepy to cool? Some options include building real-time consent into their business processes, investing in technology to support User Managed Access and privacy by design, and using digital personas to provide products and services.

Innovative data strategy options



[2] Ira Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 5 October 2012, International Data Privacy Law (2013 Forthcoming); NYU School of Law, Public Law Research Paper No. 12-56. Available at SSRN: https://ssrn.com/abstract=2157659 or http://dx.doi.org/10.2139/ssrn.2157659.

Real-time consent[3]

A leading-class strategy in building customer trust is transparency during the consent process. This includes giving customers access to means that allow them to exercise control over the use of their personal data at the time the data is used.

In addition to emphasizing key elements such as the purpose, use and disclosure of the personal information and opt-out options, online privacy notices should include manageable and accessible layers of information. Presenting information in a layered format helps make better sense of lengthy, complex information by presenting a summary of the key highlights up front. In addition, this information should remain available to individuals as they engage with the organization in case they want to reconsider whether they wish to continue or withdraw their consent.

Organizations should also design innovative processes that can be implemented just in time, are specific to the context and are appropriate to the type of interface used.

- **"Just in time" notices:** Relevant privacy information should be presented up front where it's clear, easy to see and easy to comprehend. For example, when asking for age or date of birth for a specific service, having an explanation button near the field that explains why that information is needed would aid in transparency.
- **Interactive tools:** Walkthrough videos that explain privacy settings and the benefit of each should be presented at the initial setup and periodically while the account stays active, especially if the setting has been turned off.
- **Customized mobile interfaces:** Educate the consumer around potential privacy issues at various points of the process.

User Managed Access[4]

User Managed Access is an OAuth-based access management protocol standard. It's designed to enable an individual to control the authorization of data sharing and access to other protected resources.

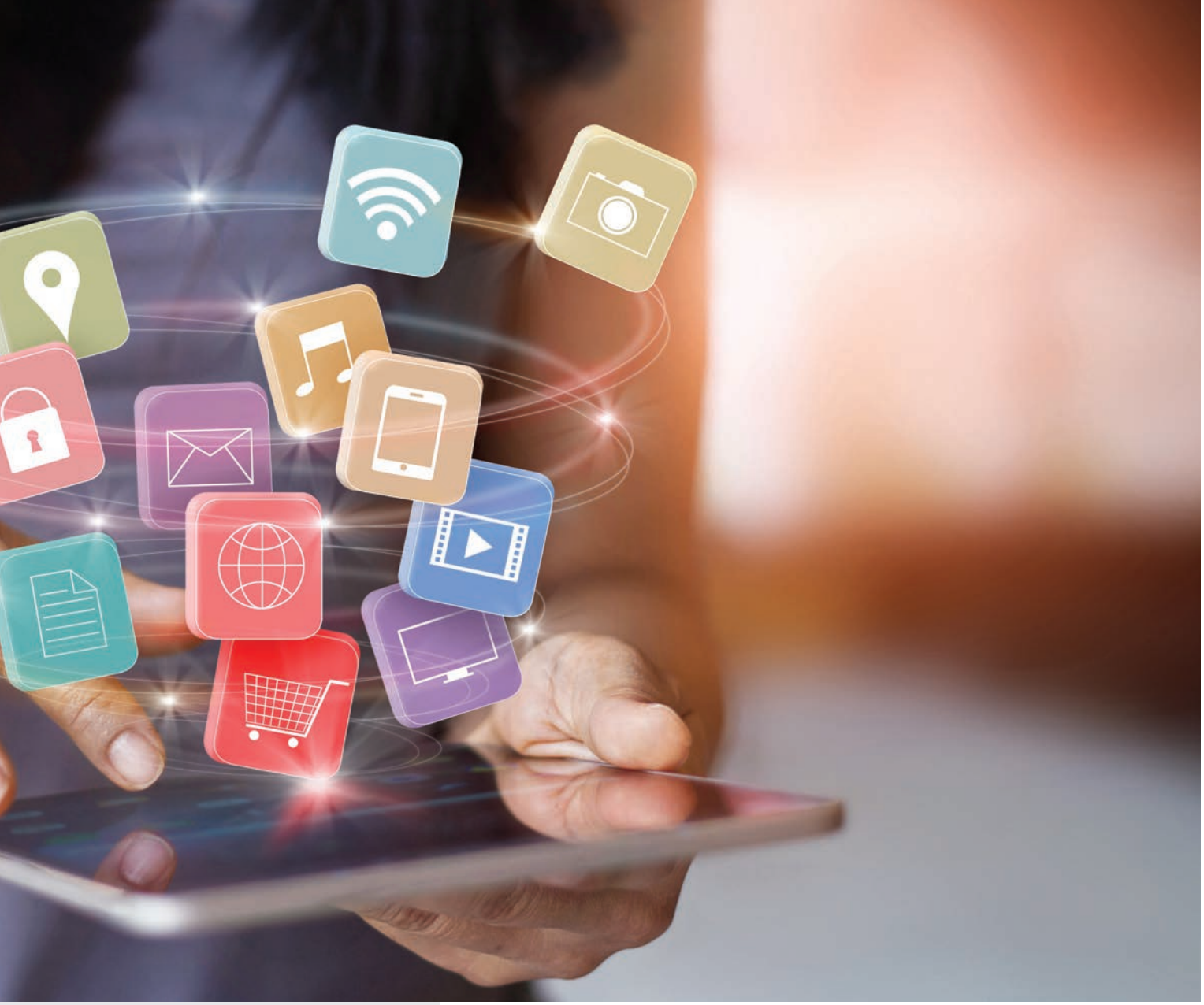
Giving users tools like User Managed Access or personal data cloud can help them understand just how much data they generate, and how it's an asset to the organization to which they're lending it. Tools like personal data vaults or clouds also let individuals organize their data around various uses (e.g., medical, social, banking). This control allows users to also assert a version of their own terms and conditions.

A best practice is for organizations to provide personal data management tools that are easy to find and use in the service interface. Specifically:

- Data management tools that make it clear who has access to a user's data and for what purpose, and, where relevant, allow the user to manage access permissions.
- Make it easier for users to remove their data from the service. (Note: GDPR requires the erasure of personal information without undue delay. This is called the right to erasure or the right to be forgotten. It may not be mandated in Canada or for services in countries outside the EU, but represents a leading-class practice to follow.)
- Create open application program interfaces to their data services so that customers can access their data and encourage them to ensure its accuracy.

[3] Office of the Privacy Commissioner of Canada, *Draft guidelines: Obtaining meaningful online consent,* 2017, accessed via https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/gl_moc_201709/, April 2017.

[4] *ISACA Journal*, "Transforming Data," Volume 6, page 20, 2017.



Privacy by design

Organizations can consider designing data protection into the development of business processes and new systems. Privacy settings are set at the highest level by default.

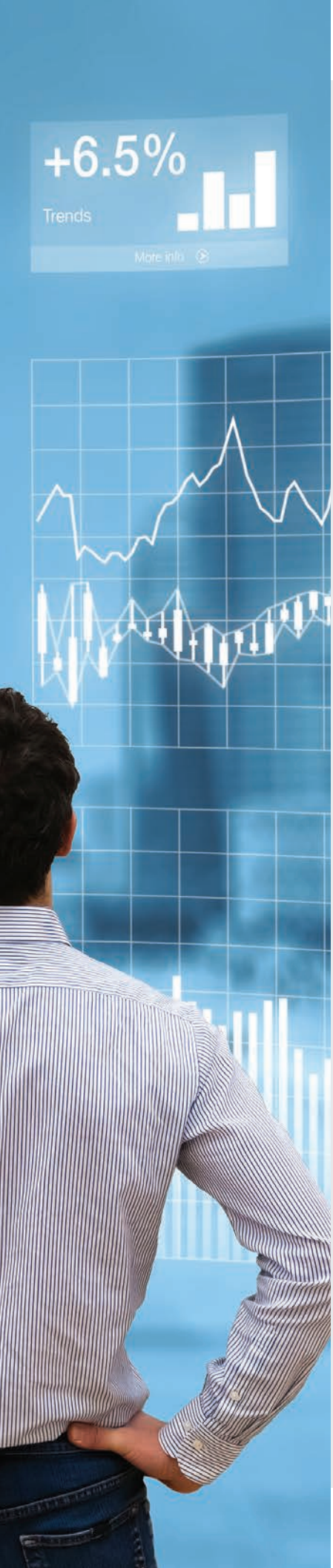
Security requirements ensure the confidentiality, integrity and availability of information that a system processes, stores or transmits. Privacy requirements advance individual privacy associated with an organization's creation, collection, use, processing, storage, maintenance, dissemination, disclosure or disposal of personally identifiable information. These requirements can be used in a variety of contexts, from policy and oversight-related activities to lifecycle-related activities that involve information systems development and engineering disciplines.

When designing a new service, protecting personal information can mean a variety of things, such as providing the user with detailed access control so they can change and verify data, creating access logs that the user can review, creating choices for the user to enable or disable what records can be accessed and by whom, and securing the logs with the user.

For designers and developers to use privacy by design or privacy by default methodologies, practical and implementable procedures must be available.

The following list outlines some leading practices around building privacy into the design stage of both the application and processes to manage the data:

- **Automatically disable accounts (or provide such options to clients) when the accounts:**
    - Have expired
    - Are no longer associated with a user
    - Are in violation of organizational policy
    - Are no longer used by applications, services or the system
    - Have been inactive for a specified period.
- **Provide the user with logs of "intended service usage" and "access to records" to enable them to become accountable:** Access to information, correction of information, records retention and destruction all have to be in the user's control, or at least the user should be able to choose these options. It's important to give users the ability to decide what to do with all the logs and documents used for troubleshooting. In other words, they should "reside" in the "domain" controlled by the user.
- **Review information flows to ensure that what was specified in the contract can be supported by the architecture of the data centres:** For example, if the data is to be contained in the EU, it should not be "archived" in the US for disaster recovery. Data flows should also be recorded in a record owned by the data or product owner.
- **Prevent encrypted information from bypassing organization-defined flow control mechanisms** by decrypting the information, blocking the flow of the encrypted information and/or terminating communications sessions attempting to pass encrypted information. Examples of flow control mechanisms include content checking, security policy filters and data type identifiers.
- **Build in controls for system outputs (exporting records, files, information):** There must be options built in for users to choose from, but with the strongest protections turned on. Allow choices for the user to enable their business models, but caution them that other controls may need to be created to protect the information extracted.
- **Consider encryption at field level for sensitive personally identifiable information as well as de-identification of personal information:** In this way, in the event of a breach, the data is incomplete and useless for any malicious intruder. Avoid or limit building fields for personally identifiable data (e.g., IP addresses) not necessary for the basic functionality of applications or processes. If you must add fields, turn off the ability to add personally identifiable information and explain to users what they're storing in the application if they turn the settings on.
- **Ensure systems have the ability to purge data at the record and field levels:** Enable information disposal from electronic repositories used for temporary transmissions or staging. A "time bomb" type of technology – or one that automatically deletes data after a period of time – would be most effective.
- **Create mini-explanations about fields or their privacy implications and embed this education in the application/product:** Embed messages or explanations for transparency about data practices, limits on the collection, storage and retention of data, meaningful choices for users, security, and your organization's accountability with respect to data protection.
- **When enhancing or implementing changes in existing applications or services, test that the previous privacy controls still work** as originally designed, that privacy options are set by default to "on" and that this is still the case after the changes are implemented.



Digital personas[5]

Privacy regulations stress the importance of collecting the minimal amount of personal information required to fulfill the original purpose for which it was needed. But what if you can take it a step further to ensure your customers' privacy? Is it possible you can provide the same services and products by using a digital persona?

A digital persona is a realistic representation of consumer groups that are based on research and data. These personas are developed using aggregated customer data from a variety of sources – such as website analytics, online surveys, social media use among others – to advise on the creation of groups of personas that represent the organization's digital customers.

Organizations should allow individuals to receive products or services using a digital persona identity where possible. In these settings, trust transactions can still be enabled without giving up the individual's "root" identity.

For example, it's possible to validate whether a user is eligible for a service based on their age instead of asking for their date of birth. Attribute verification will play a significant role in enabling individuals to select the identity that provides access without compromising the individual's capacity to act independently and exercise free choice.

Summary

Big data business strategy

+

Customer-focused data privacy strategy

=

Competitive advantage

The pace of business transformation is rapid for most organizations, driven by market insurgents, new customer demands, technology innovation and other factors. To stay competitive, leading enterprises are using advanced analytics to improve current business processes and answer the fundamental question, "What's next?" when it comes to what to sell, how to sell, who to sell to, and how to outflank the competition. Those that are not making progress quickly enough are at an increased risk of falling behind both current competitors and emerging players that were "born" digital with advanced analytics at the centre of their strategy.[1]

Organizations that strategize the use of advanced analytics, also need to seek a forward-looking data privacy strategy that incorporates customer rights, ethical use of data, and legal and compliance obligations. This will give organizations a competitive advantage in building trusted relationships with their customers while reaping the significant economic and social benefits of advanced analytics.

[5] Ethically Aligned Design, IEEE full document, December 2017, Version 2.

Contacts

Alex Mohelsky
Partner,
National Analytics leader
Toronto
416 943 2347
Alex.Mohelsky@ca.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients.

For more information about our organization, please visit ey.com/ca.

2669545
ED 0000

ey.com/ca