WORLD ECONOMIC FORUM

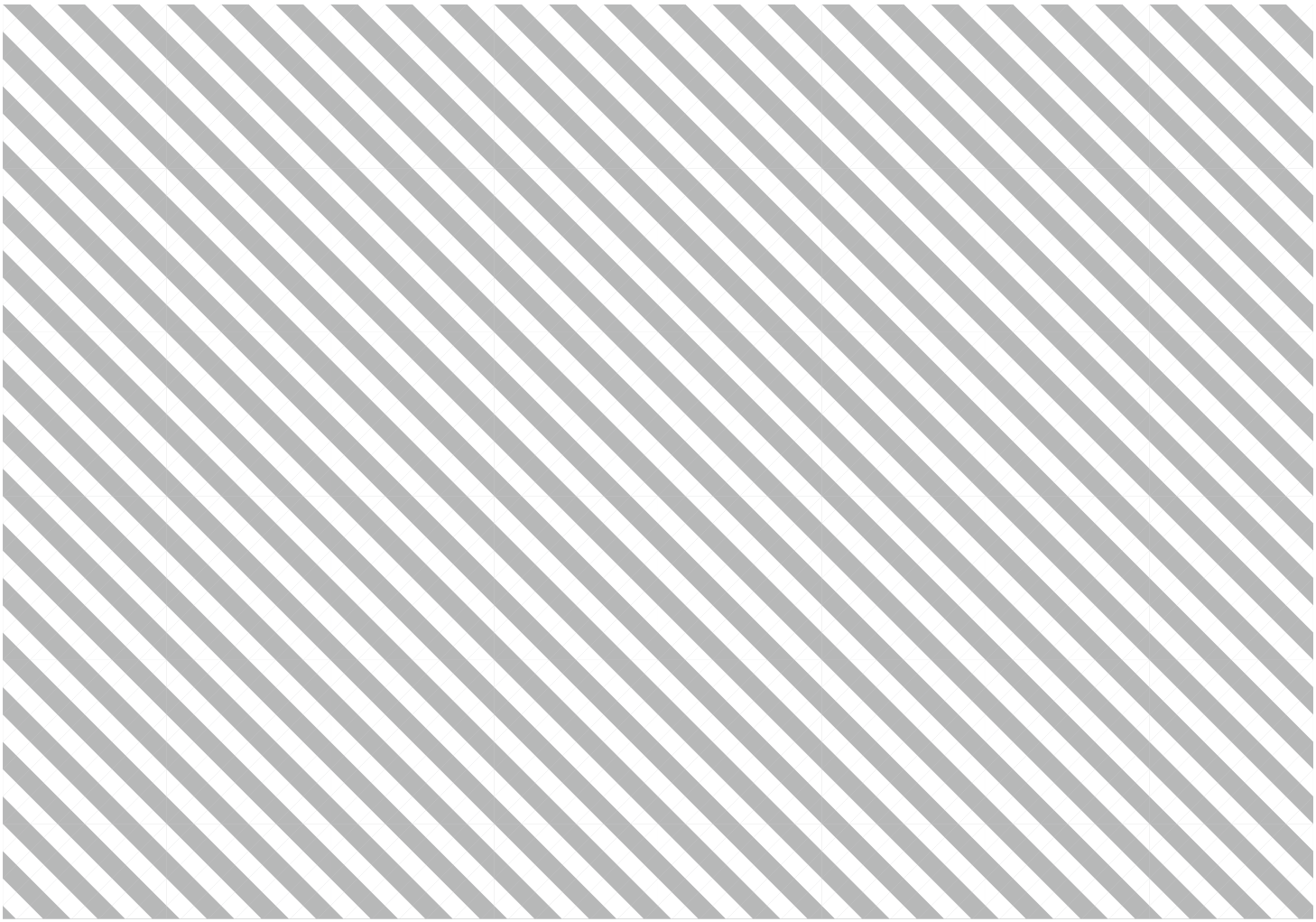
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

The Appropriate Use of Customer Data in Financial Services

Prepared in collaboration with Oliver Wyman

September 2018



Contents

World Economic Forum®

REF 160418 - case 00048540

Executive summary

In an effort to understand better the implications of the Fourth Industrial Revolution – a technology-led transformation that is fundamentally altering the way people work, live and relate to one another – the World Economic Forum prioritized a review of the financial system through its initiative, Balancing Financial Stability, Innovation and Economic Growth. A key part of this review focused on the appropriate use of customer data in financial services.

This review began a year ago and several developments since have reinforced the urgency of this work. Whether it is data breaches at large organizations crucial to the provision of credit, disclosures of controversial data-sharing practices at social media firms offering payment services, or considerations by big techs to partner with banks and exchange customer and transaction data, the accelerating data-fuelled transformation of financial services demonstrates the need for stakeholders to align on principles governing the use of customer data. Uncertainty about what it means to use customer data appropriately could cause a loss of trust that could lead to instability in the financial services system.

Policy-makers recognize the need for guidance and have been implementing legislative responses, most notably through the European Union's General Data Protection Regulation (GDPR). California and China have passed similar laws and numerous jurisdictions are currently formulating or reviewing their respective data regulations. These necessary efforts introduce important checks and balances, yet are insufficient. An uncoordinated proliferation of global data frameworks may prove counterproductive in the long run, resulting in further regulatory fragmentation with adverse knock-on effects for innovation and new business formation.

Through a series of roundtable discussions and interviews with industry executives and experts across multiple regions, the Forum stakeholders identified the lack of global principles to guide the inherent trade-offs to be made in the use of customer data as a major foundational gap. A draft set of global principles has been developed and the Forum stakeholders encourage their adoption. The principles, focused on control, security, personalization, advanced analytics and portability, demonstrate the feasibility of achieving high-level consensus on customer data collection and use practices globally.

The consequences of inaction on the appropriate use of customer data – such as overexposure to risk, the stifling of innovation, or competitive inequity leading to poor industry structure – demand the expedited, yet careful, implementation of these principles globally. To address the range of practical implementation challenges, the principles suggest a series of next steps for governments, incumbents and challengers. By following the roadmap developed to tackle these obstacles, stakeholders can better manage the trade-offs of using customer data and addressing key data-related challenges – ultimately, balancing financial stability, innovation and economic growth.

This document builds on the **Balancing Financial Stability, Innovation and Economic Growth** White Paper published in June 2017, which made the following findings:

1. **Major innovation-driven change is coming to financial services.** Firms are increasingly competing or partnering at different points along the financial services value chain to take advantage of unmet customer needs, less efficient cost structures, high capital usage and attractive returns.
2. **These changes can bring enormous benefits to the financial services system.** Benefits include improved customer experience, better risk management and greater efficiency for incumbent industry participants and new value creators.
3. **Managing some systemic risks introduced by this wave of innovation poses challenges.** The appropriate use and competitive advantage of customer data was identified as a key area of focus by the Stewards of the Forum System Initiative on Shaping the Future of Financial and Monetary Systems and the Steering Committee of the Balancing Financial Stability, Innovation and Economic Growth initiative.
4. **The financial services system would benefit from certain tools to achieve greater enablement and risk management.** These include a more standardized regulatory treatment framework across jurisdictions.

Using data to build a better financial system

1 Customer data are critical to innovation and growth, but data misuse risks a loss of trust that could destabilize the financial services system

Customer

- ✓ New products and services tailored to individual needs
- ✓ Enhanced customer experience
- ✓ Financial inclusion for underserved individuals
- ✗ Financial losses due to fraud
- ✗ Loss of privacy if data are used without consent
- ✗ Exclusion from products or services due to real or perceived risks

Business

- ✓ Development of new products and services
- ✓ Better risk management capabilities
- ✓ Cost savings from more efficient internal operations
- ✗ Regulatory penalties or reputational damage from misuse of customer data (loss of customers)
- ✗ Operational losses from fraud or cyberattacks
- ✗ Market disruption for companies that depend on pooled risk or cross-subsidization

2 Stakeholder discussions identified five challenges to reach consensus on the appropriate use of customer data in financial services

Challenge 1:
Varying stakeholder incentives regarding the use of customer data

Challenge 2:
Regional differences around the world in societal and cultural beliefs concerning customer data

Challenge 3:
Complexity of different data types, uses and collection approaches

Challenge 4:
Lack of common principles for framing issues

Challenge 5:
Issues of practical regulation and implementation of shared principles

3 Governments, incumbents and challengers need to take action in 10 key areas to ensure the financial system evolves appropriately

Governments

1. **Enable global coordination on principles** for the appropriate use of customer data
2. **Establish legal and regulatory safeguards** that balance customer data oversight and innovation
3. **Ensure supervisors have the tools and expertise** to provide effective oversight of customer data
4. **Develop customer data critical infrastructure** and associated standards and protocols

Incumbents

5. **Strengthen trust** with customers and regulators by proactively addressing data privacy, security and appropriate use
6. **Deepen customer relationships** by focusing on long-term data stewardship over short-term commercial incentives
7. **Collaborate with other incumbents and challengers** to demonstrate industry leadership on customer data

Challengers

8. **Meet or exceed expectations** from customers and regulators to provide financial products and services
9. **Manage risks** associated with using new types of customer data or advanced analytics
10. **Protect customer data** while maximizing growth and value creation

Source: World Economic Forum and Oliver Wyman

Global customer data principles

Control

"Companies should be clear about their use of customer data, attain customer agreement to their customer data policies and, where appropriate, seek consent for specific uses."

What is meant by control?

Control refers to the **relative ability** of businesses and consumers **to use and capture value from data.**

Key questions:

- *When is consent required to use customer data?*
- *What is required for informed consent?*
- *Can customers request to know the data about them held by companies?*

What conditions are required to be effective in practice?

- **Informed consent:** Companies need to provide clear and accessible information about how customer data will be used (e.g. terms and conditions).
- **Transparency:** Customers should be able to view or know the data that are collected about them, how they are used and whether they are shared with a third party.
- **Ability to revoke consent:** Customers should be able to request that data about them no longer be used by an organization (e.g. the right to be forgotten).
- **Legitimate use:** Companies may not need to seek consent when using data for legitimate interests (e.g. those required by law).

Security

"Companies should be held responsible and accountable for data security."

What is meant by security?

Security refers to how **data security responsibility** is balanced between customers and companies.

Key questions:

- *What responsibilities do companies have to secure customer data?*

What conditions are required to be effective in practice?

- **Liability:** A clear liability framework should be in place that ensures the responsible party is held accountable for data security and for harms caused by breaches of its respective data security duties of care.
- **Traceability:** Companies need to be able to identify where data were improperly used or accessed in the event of a security breach.

Personalization

"Companies should be able to create individual customer-level profiles that allow them to provide differentiated customer services."

What is meant by personalization?

Personalization refers to whether companies can provide **differentiated services** to customers.

Key questions:

- *Should businesses treat people equally or as individuals?*
- *To what extent should companies incorporate customer preferences for data use?*

What conditions are required to be effective in practice?

- **Intervention:** Customers should be able to intervene to gain information or limit the use of data they control, and companies should respond appropriately.
- **Limited use:** Where reasonable, a maximum time period that data can be retained by companies should exist, as well as limits on certain sensitive data types or uses.

Advanced analytics

"Companies should be able to comprehensively test, validate and explain their use of data analytics and models to customers."

What is meant by advanced analytics?

Advanced analytics refers to whether **safeguards** are needed to use **new models and statistical approaches**.

Key questions:

- *Are safeguards necessary to prevent data from leading to discrimination and exclusion?*
- *Should customers have the right to correct or update data about them?*

What conditions are required to be effective in practice?

- **Justification:** Customers should have the right to request why a decision was made (e.g. why the model methodology is appropriate, why the output is justified).
- **Challenge:** Customers should have the right to correct incorrect or incomplete data about them held by a company.

Portability

"Companies should, where appropriate, allow customers to access, download, transfer and/or permit third parties to manage data about them."

What is meant by portability?

Portability refers to the **ability of customers to transfer data about them** between private-sector participants.

Key questions:

- *Who should be able to authorize the transfer of customer data between private-sector participants?*
- *Do data formatting standards need to be created?*

What conditions are required to be effective in practice?

- **Accessibility:** Companies should allow customers to download data about them in machine-readable format or through standardized APIs, depending on companies' stage of development and jurisdiction.
- **Third-party permissions:** Accessibility encompasses customers giving third parties permission to download their data.

Source: World Economic Forum and Oliver Wyman

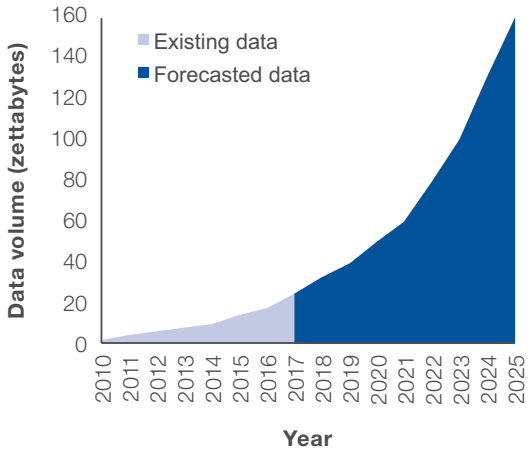
Background

The generation of data has exploded, with the global volume of data predicted to double from 2018 to 2022 (Figure 1). While data are having a transformative effect across industries, this paper focuses on the role of data in financial services, where incumbents (large, successful companies that predate the digital revolution) as well as financial technology (fintech) and large technology firms are rapidly increasing their abilities to collect and use data about the people using their products and services (customers).

Technological innovations have improved the ability of businesses to capture and use customer data. Internet-of-things technologies allow companies to collect a greater variety of customer data, such as customer locations and behaviour. Advanced computing increases the ability to store, manage and transfer data, while advanced analytics permits greater insight into customer behaviours and preferences (Figure 2).

These innovations have created opportunities for business innovation. They have also led to uncertainty, however, about what it means to use customer data appropriately. Governments around the world are debating whether to adopt elements of Europe's new General Data Protection Regulation (GDPR). Business leaders are considering what they would do if a third party misused customer data. And finally, customers are asking how companies are collecting, using and sharing data about them, and what benefits they are getting in return.

Figure 1: Annual global data volume



Certain marketing companies have about **1,500 data points** on approximately **96%** of US citizens

95% of the top free mobile apps collect customer data (location, social networks, etc.)

Note: Data points are units of observations or characteristics (e.g. gender, location, ethnicity) related to the referenced citizens.

Sources: Reinsel et al. (2017), CitiBank (2017)

Figure 2: Impact of technological innovations on customer data

Technology	Description	Examples of customer data impact
Digitization	Electronic housing of customer information and digital interface to facilitate information processes	Collection of a greater variety of customer data, such as purchase history and web browsing time
Internet of things	Network of internet-connected objects able to collect and exchange data using embedded sensors Collection of customers' locations and behaviours	Secure verification of customers' identity
Biometrics	Identity authentication through use of uniquely physical or behavioural characteristics (e.g. facial recognition, fingerprints, voice recognition)	Secure verification of customers' identity
Advanced analytics/ artificial intelligence	Statistics and modelling used to determine future performance based on current and historical data	Data mining to provide better insight into behaviours and preferences
Robotics	Software solutions that automate routine, repetitive or rule-based processes	Reduction of operational costs for consuming, manipulating and acting on customer data
Advanced computing (quantum, edge, cloud, mobile)	Network of remote servers hosted on the internet; systems based on quantum effects; devices created using mobile components; optimization from performing data processing at the edge of the network	Increase in ease of storing, managing, transferring and processing data
Open application programming interfaces (APIs)/ microservices	Publicly available API that provides access to a proprietary software application or web service	Secure sharing of data with reduced risk of breach
Distributed ledger technology (blockchain)	Public transactions enabled through a database consensually shared among networks spread across multiple sites, institutions or geographies	Customers regaining control of personal data, including access and transfer
Advanced encryption	Advanced encryption methods, such as zero knowledge proofs and tokenization of data	Development of alternative approaches to sharing personally identifiable information

Source: World Economic Forum and Oliver Wyman

Opportunities and risks

The opportunities and risks in customer data (Figure 3) have implications for the global financial services system. Both customers and businesses deserve the opportunity to benefit from the expanded use of such data. For these benefits to be realized, however, customers need to trust that data about them will be used appropriately, and that they will share in the value created.

Companies can design products and services customized with customers' individual data. Most financial products and services are standardized, making it difficult for businesses to meet the unique needs of their customers – people with diverse financial circumstances who may want to study at a university, buy a house or start a company. Expanded use of customer data can help companies design cheaper and better services, such as targeted insurance products for gig-economy workers with varying income over time, or customized loan products for businesses with seasonal sales.

The opportunities for customer data to create value for both businesses and customers are enormous. In addition to better products and services, the expanded use of this data can increase economic growth by bringing new customers into the financial system. This is particularly true for many customers in developing countries, where alternative data sources can allow for greater access to savings accounts and credit products.

However, failing to protect customer data appropriately means companies face significant risks. Protecting customer data is challenging: data can be misused by bad actors within a company, stolen by cybercriminals or inappropriately shared with third parties. Data misuse can lead to direct financial losses, due either to an increase in fraud claims or regulatory fines. Companies that fail the "newspaper test" (i.e. the implications of their misusing data when such practices are publicized) can also face significant reputational consequences.

Customer data may also pose risks to market stability because of changing economic incentives. Increased availability of more granular customer data could encourage companies to focus on their most profitable customer segments. This could lead to disruption in markets that depend on pooled risk or cross-subsidized products and services. In parallel, customers could be excluded from using products or services due to real or perceived risks.

Finding consensus on the appropriate use of customer data is critical to balancing financial stability, innovation and economic growth. While a lack of customer data safeguards can weaken trust, over-regulation can also hinder innovation by restricting development of products and services that customers want. Managing key trade-offs and identifying areas of common ground will be critical to ensuring the benefits of customer data are realized across the financial services system.

Figure 3: Customer data opportunities and risks

Customer

- ✓ New products and services tailored to individual needs
- ✓ Enhanced customer experience
- ✓ Financial inclusion for underserved individuals
- ✗ Financial losses due to fraud
- ✗ Loss of privacy if data are used without consent
- ✗ Exclusion from products or services due to real or perceived risks

Business

- ✓ Development of new products and services
- ✓ Better risk management capabilities
- ✓ Cost savings from more efficient internal operations
- ✗ Regulatory penalties or reputational damage from misuse of customer data
- ✗ Operational losses from fraud or cyberattacks
- ✗ Market disruption for companies that depend on pooled risk or cross-subsidization

> "The dignity of the human person, and a healthy community, can be protected only if the expansion of economic opportunity is balanced with human rights and respected mutual responsibilities. Big data can deliver improved financial support for people, especially benefiting the previously 'unbanked' poor. But it must not exploit the ignorant, the naïve and the marginalized. Big data and artificial intelligence should not produce diminished life opportunities and constrained autonomy for the minority. A healthy community cannot be achieved where microdata analysis results in groups being excluded from banking or insurance services merely in the name of targeted profit maximization."

Bishop Paul Tighe, Secretary of the Pontifical Council for Culture, The Vatican

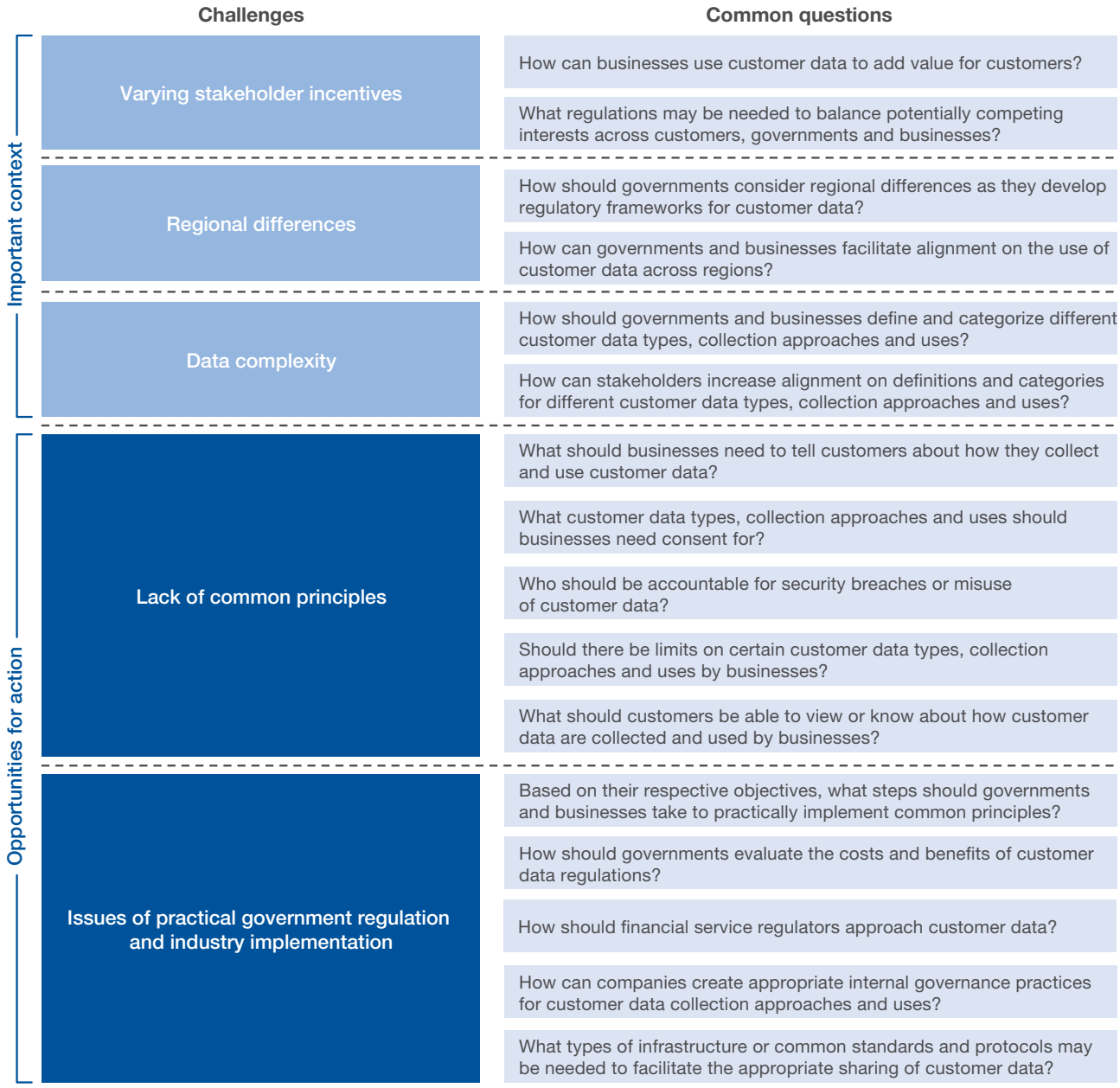
Customer data challenges

Five major challenges (Figure 4) make it difficult to gain consensus on the appropriate use of customer data:

1. **Varying stakeholder incentives** regarding the use of customer data across customers, governments and businesses
2. **Regional differences** around the world in societal and cultural beliefs concerning customer data
3. **Complexity** of different data types, uses and collection approaches, making it challenging to create consistent standards and practices
4. **Lack of common principles for framing issues** concerning the appropriate use of customer data across topics such as liability, consent and transparency
5. **Issues of practical government regulation and implementation of shared principles** across governments and the financial services industry

Each of these key challenges comprises common questions underpinning global conversations and debate about the appropriate use of customer data, particularly in the financial services sector.

Figure 4: Customer data challenges



Source: World Economic Forum and Oliver Wyman

1. Varying stakeholder incentives

Customers, governments and businesses have specific and sometimes competing interests regarding customer data (Figure 5).

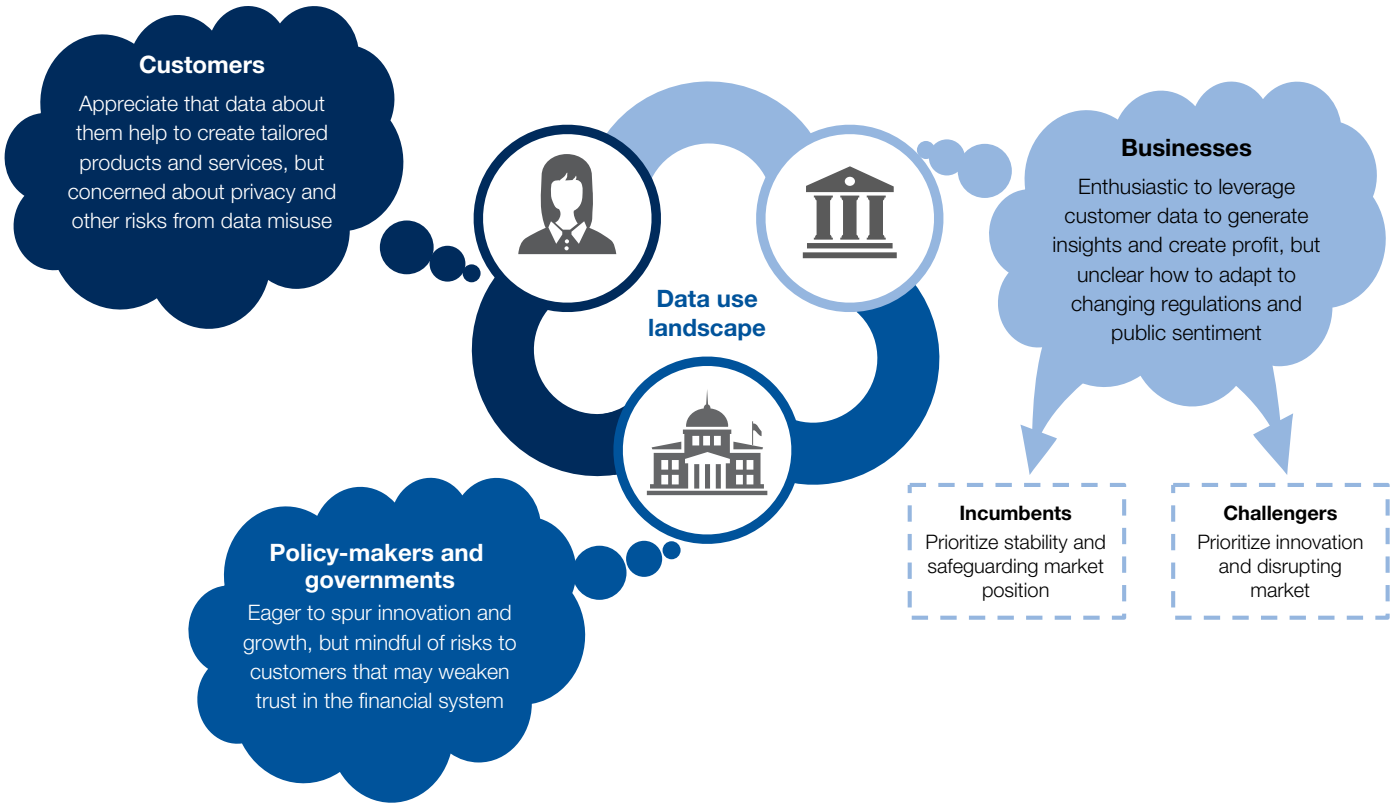
Customers appreciate that data about them can be used to create tailored products and services but are concerned about privacy and misuse of that data (Figure 6). Customer data have allowed businesses to streamline applications for many financial products and services, saving time and enhancing the customer experience. Customers also have gained access to innovations based on both personal and aggregated customer data. However, many of them are concerned about data authenticity and the impacts of data misuse, from the growing number of automated telemarketing phone calls to issues about fraud and identify theft.

Governments are eager to spur innovation and growth but are concerned about risks that may weaken trust in the financial system. While regulators around the world are experimenting with new tools and approaches, they struggle with how to address products and services that fall outside existing regulatory frameworks. The pace of technological advances means that existing laws and regulations can quickly become obsolete, frustrating both customers and businesses seeking to access new innovations. However, customers can also become concerned if they feel governments are not sufficiently protecting them from new risks.

Incumbents are eager to leverage customer data but prioritize stability and safeguarding their market position. Incumbents – large, successful companies that predate the digital revolution – are investing in their data infrastructure and actively working to enhance their offering of digital products and services. Many firms, however, face significant challenges in upgrading their legacy technology systems. Incumbents also need to address new market entrants, as well as changes required by new and pending regulations.

Challengers prioritize innovation and growth while adapting to changes in public and regulatory attitudes. Challengers within financial services, particularly small fintech firms, often focus on gaining access to larger markets, which increasingly involves partnering with incumbents. Challengers outside financial services, particularly established technology firms, are also considering offering financial products and services directly (business to consumer) or to other financial services companies (business to business). Both types of challengers must adapt to the regulatory environment and consider whether and how to partner with incumbents.

Figure 5: Customer data stakeholders



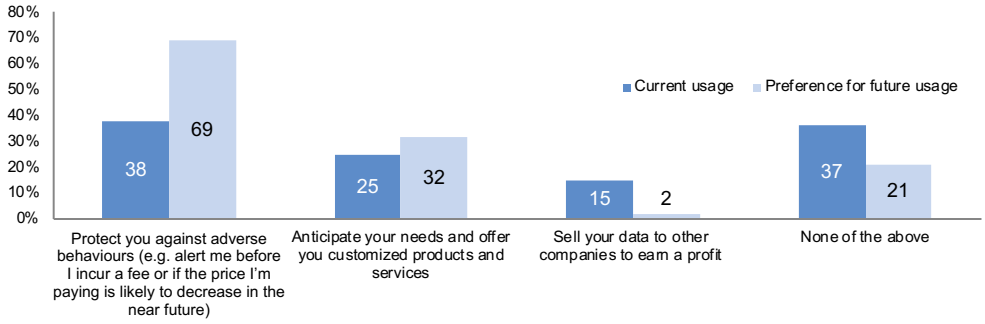
Source: World Economic Forum and Oliver Wyman

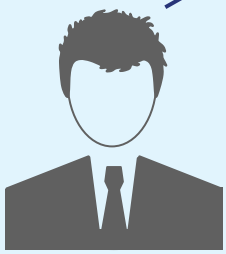
Figure 6: Customer views on how companies should handle their data

Customers want financial institutions to use data about them in ways that they can benefit from

- Most customers are uncomfortable with smartphone and tablet apps using their personal data and are worried that sharing data makes them targets for marketing campaigns
- **84%** of those surveyed feel they have less than sufficient control over the way organizations use data about them

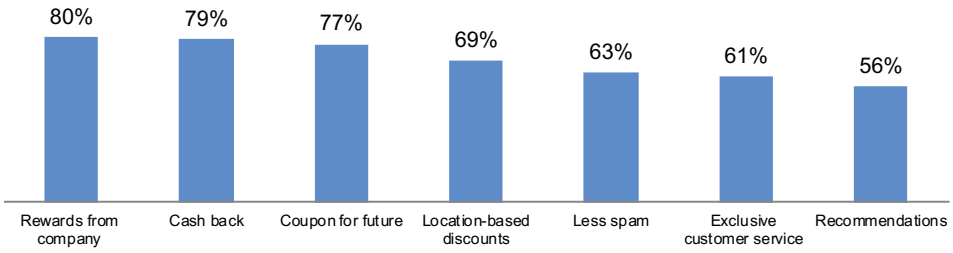
How do customers want financial institutions to use their data?[1]





Customers are often willing to share data for free or discounted products

- **50%** would accept free or discounted products in exchange for less privacy, including **45%** who would allow their automobile driving habits to be monitored to receive cheaper insurance premiums
- Customers are willing to share a non-required piece of data[2] for various benefits, including:



Customers are more willing to share data with brands they trust[3]

- **75%** are more willing to share personal data with a brand they trust
- **48%** would lose trust in their bank and **28%** would switch to a new bank if their bank were accused of unethical business practices that did not impact them personally

[1] The question in the Oliver Wyman 2017 Trust Survey of about 4,800 US adults was: "How do you think that your primary bank currently uses your less sensitive personal and account history data (e.g. contact info, purchase history, etc.)? How would you prefer that the company use your less sensitive personal and account history data in the future? Please select all that apply."

[2] A non-required piece of data refers to personal information not required to receive the service. The results shown are from a 2015 survey by the Center on Global Brand Leadership at Columbia Business School, in conjunction with Aimia, of over 8,000 consumers across four generations in five countries (United States, Canada, United Kingdom, France and India). See Quint and Rogers (2015).

[3] Results are also from the 2015 survey. See Quint and Rogers (2015).
Sources: European Commission (2015); CitiBank (2017); Morey et al. (2015); Cooper and LaSalle (2016); KPMG (2017); Oliver Wyman (2017); Quint and Rogers (2015).

2. Regional differences

Although stakeholder perspectives are important, significant differences exist in beliefs and regulations concerning customer data around the world. While more than 120 countries have enacted data protection legislation, this paper highlights three distinct regional approaches:

- **Europe** recently established the GDPR, an overarching data protection law that provides strong personal data protections and enhances residents' rights to data about them.
- In the **Americas**, and particularly the United States, numerous sectoral laws are aimed at preventing physical and/or economic harm rather than codifying data protection as a fundamental right.
- Countries in **Asia-Pacific**, with comparatively less focus on individual data ownership rights, have focused on balancing economic development and financial inclusion with the need to protect sensitive data.

Understanding regional differences is important because customer data increasingly crosses political boundaries. In the past, companies were often subject to regulation in a single jurisdiction. Now, they may need to account for their customers' locations, their data storage centres and data processing facilities when considering what regulations will apply to their activities. For companies that leverage multiple cloud-based service providers, even identifying the appropriate jurisdictions may be challenging.

Europe

Europe has enacted comprehensive data protection and open banking legislation that views protection of data as a human right. The GDPR requires companies that are based in the EU, process data in the EU or do business with EU customers to examine their data usage practices and remediate gaps to avoid financial penalties. The GDPR reinforces data protection requirements and establishes new individual rights (8), including data portability and the right to be forgotten. For open banking, the revised Payment Services Directive (PSD2) requires banks to provide access to customer bank account information and payment initiation to third-party providers, provided customers consent to this.

Figure 7: Europe and the implications of GDPR

GDPR data principles[1]	
Lawfulness, fairness and transparency	Data should be processed **lawfully, fairly and in a transparent manner** in relation to individuals
Purpose limitation	Data should be collected for s**pecified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes
Data minimization	Data processing should be **adequate, relevant and limited** to what is necessary
Accuracy	**Data should be accurate and**, where necessary, **kept up to date**
Storage limitation	Data should be kept in a form that **permits identification** of data subjects **for no longer than is necessary**
Integrity and confidentiality	Data should be processed in a manner that ensures **appropriate security for personal information**
Accountability	**The controller should be responsible** for, and be able to demonstrate compliance with, **the principles above**

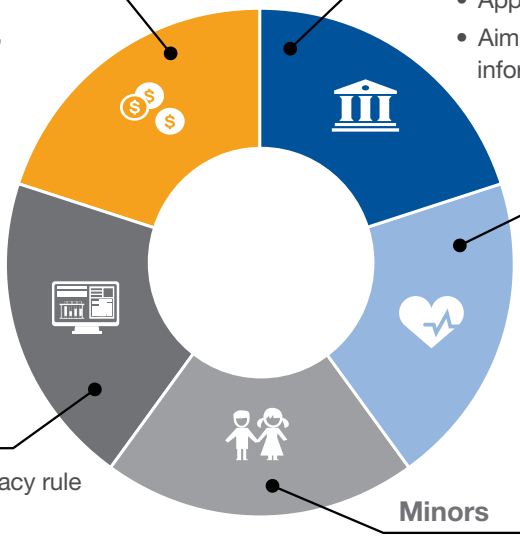
Key implications of GDPR
1. **Increased territorial scope** as GDPR applies to all companies that process data on EU residents
2. **Stricter penalties requiring compliance**, with revenue-based fines (≤ 4% of annual global turnover or €20 million), broad supervisory powers and greater risk of private claims
3. **Strengthened consent conditions** requiring clear and accessible forms, as well as greater ease to withdraw consent
4. **Wider data scope** as "personal data" and "special categories" of personal data (sensitive personal data) defined more broadly
5. **Expanded rights of data subjects**, including the right to have data erased and the right to have data transferred to another controller (data portability)
6. **Privacy by design/default**, such that privacy might be considered throughout the product development process, and that companies default to strict privacy settings
7. **Appointment of data protection officers** who must adhere to internal record-keeping requirements
8. **Regulation of suppliers (data processors)** and controllers
9. **Mandatory notification of data breaches**
10. **Higher bar for lawful processing of data**
11. **Increased accountability measures**

1 General Data Protection Regulation (GDPR), Article 5: Principles relating to processing of personal data.
Sources: European Union Agency for Fundamental Rights (2017); Allen & Overy (2018); DLA Piper (2017); Accenture, Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2 (2016); Wintermeyer (2017); Bowcott (2017); CitiBank (2017)

Americas

Sector-specific legislation in the Americas, and particularly the United States, regulates the use of personal data within industries (Figure 8). On a federal level, the Gramm-Leach-Bliley Act applies to financial institutions and to businesses that provide financial products and services. In terms of enforcement, the Federal Trade Commission (FTC) promotes consumer protection of personal data and can investigate and address a company's failure to comply with their own privacy practices. It is important to note, however, that despite these regulations, the United States does not have a comprehensive national data privacy or use policy. In light of this, states are independently developing legislation. In mid-2018, California passed the California Consumer Privacy Act of 2018, changing requirements for how businesses in the state handle data and setting a precedent for other states' consideration.

Figure 8: US federal legislation on customer data



Financial institutions

- Gramm-Leach-Bliley Act enacted in 1999
- Dodd-Frank Act, Section 1033, requires financial institutions to provide customers with copies of data about them
- CFPB has issued principles on financial data sharing and aggregation
- Several FTC rules regulate protection and disposal of financial data

Credit reporting

- Fair Credit Reporting Act
- Applies to consumer reporting agencies
- Aims to protect consumers from inaccurate information on credit reports

Healthcare

- Health Insurance Portability and Accountability Act and associated rules
- Applies to all entities that handle protected health information
- Regulates the collection, use and protection of PHI

Internet service providers

- April 2017 repeal of FCC's privacy rule for broadband ISPs
- FCC privacy rule included browsing history and app usage as sensitive data and detailed customer consent requirements
- Repeal of regulation enables ISPs to sell data without customer consent

Minors

- Children's Online Privacy Protection Act applies to websites collecting data on children under 13 years of age
- Regulates privacy policies, obtainment of consent and website operator's responsibility to protect children's privacy and online safety

Notes: CFPB = Consumer Financial Protection Bureau; FTC = Federal Trade Commission; FCC = Federal Communications Commission; ISP = internet service provider; PHI = protected health information.
Sources: Jolly (2017); King and Raja (2013); Raul (2016)

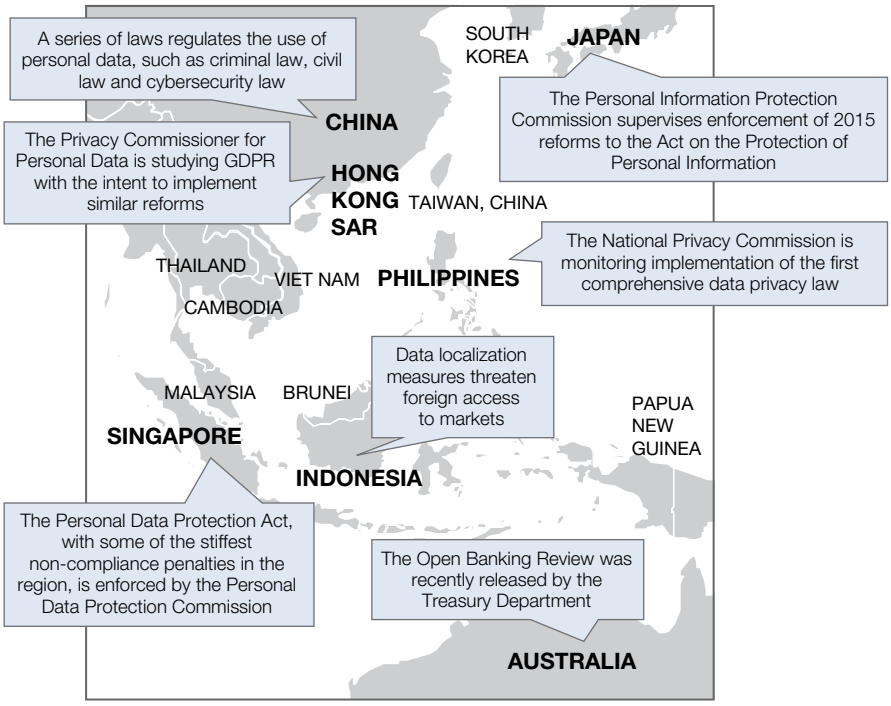
> **Data-driven products and practices could be a powerful force for financial inclusion and efficiency, but they will only be used if they achieve consumers' trust. Financial service providers need to demonstrate that data is being collected, stored and used in a way that aligns with their customers' interests – regardless of where the data comes from.**

Greg Medcraft, Director, Financial and Enterprise Affairs, Organisation for Economic Co-operation and Development (OECD), Paris

Asia-Pacific

Asia-Pacific countries have increasingly focused on strengthening data protection (Figure 9) while enabling economic growth. Although some ongoing efforts seek to harmonize data protection regulation in the region, varying political agendas and levels of expertise pose challenges to developing a comprehensive regulatory framework. Key considerations for regulators include whether to align regulations with GDPR, how to balance financial inclusion with the need to protect sensitive data, and the role of government. An example of these ongoing considerations, China's recent data protection law taking effect in May 2018 laid out broad principles on personal information protection but left key issues related to scope and implementation unresolved, to be filled in as a further understanding of issues like interoperability is brought to light.

Figure 9: Asia-Pacific regulatory developments



Sources: Hogan Lovells (2017); Raul (2016); DLA Piper (2017); ADMA (2017)

3. Complexity across data type, collection approach and use

The three key dimensions for customer data are data type, data collection approach and data use. They have important implications for questions about the appropriate use of data in financial services, as well as the competitive advantage associated with data.

Figure 10: Traditional and emerging types of customer data

	Traditional forms	Emerging forms
Identity	Public records, tax filings	Fingerprints, photographs, iris scans, digital IDs
Health	Medical records, insurance claims	Fitness tracking, sleep/eating habits
Financial	Bank statements, credit scores	Peer-to-peer payments, online budgeting
Social	Organization registries	Social media connections and activities
Location	Telephone books	Geolocation tracking
Media behaviour	Library checkout histories	Web browsing activities, content streaming

Source: World Economic Forum and Oliver Wyman

Data type: Historically, customer data included paper-based records (Figure 10) that served a single purpose and changed slowly over months and years. Sensitive personal data, such as a person's social security number or bank statements, were relatively easy to define and protect.

Customer data currently includes real-time electronic data with few industry barriers. Data aggregators can collect data from numerous sources to create customer profiles, or to predict data that could be considered sensitive, such as a person's financial or health status, or biometric information.

Data collection approach: Customer data can be volunteered by customers, observed from customer behaviour, inferred by companies or obtained from third parties. For example, a customer with a mortgage from a bank would provide volunteered data in the application form, such as their demographic data and income. The customer's loan payment history would be considered observed data, while data from the bank's underwriting models on the size of the loan they qualify for would be inferred data. The bank could also seek out observed or inferred data from third parties, such as the customer's credit score (Figure 11).

Figure 11: Data collection approaches

	Definition	Examples
Volunteered data	Explicitly provided by customer	Demographic data, self-reported income
Observed data	Created through customer activity	Transaction history, web browsing history
Inferred data	Proprietary forecasts using other data types	Underwriting output, customer profiles
Third-party data	Purchased by institution	FICO credit score, background check

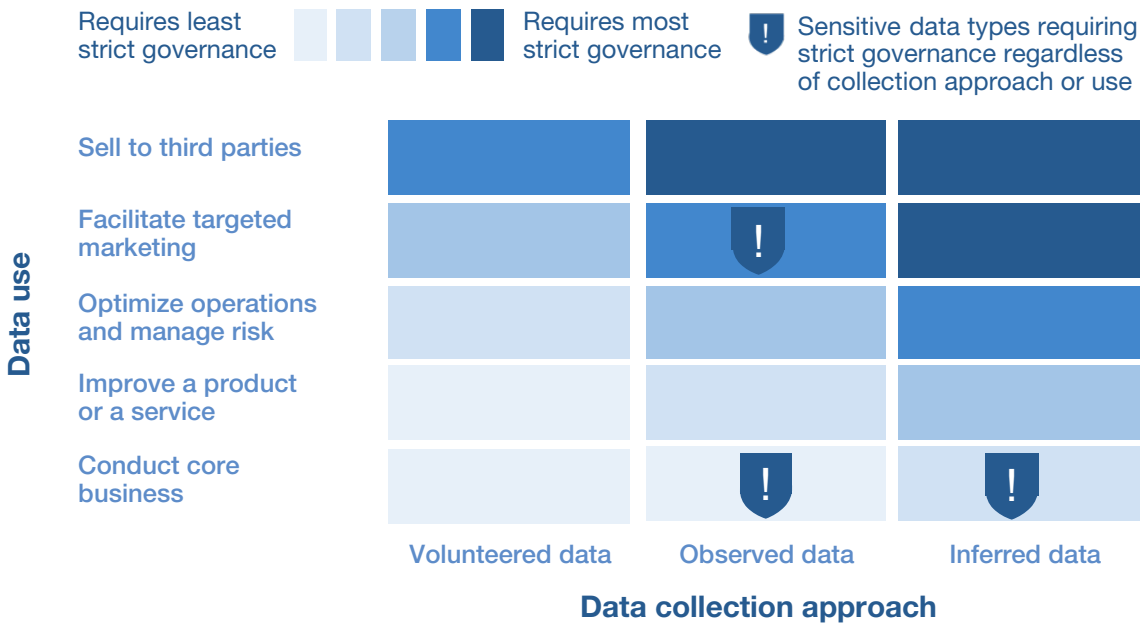
Note: FICO refers to the Fair Isaac Corporation, which created the credit score. Source: World Economic Forum and Oliver Wyman

Data use: Customer data can be used for a variety of purposes, including core business processes, improving products or services, risk management and marketing, or can be shared with third parties. The same data can sometimes be used for multiple purposes – for example, leveraging existing transaction data to develop new products or target new customers through marketing. Selling or transferring data to third parties can also occur for multiple purposes, either because the data are needed to operate the third party or to monetize the data's value. Finally, some data uses are also mandated by law, such as anti-financial-crime reporting requirements.

As businesses and governments design data governance frameworks, some data types, collection approaches and uses may require stricter oversight. For example, financial or health data may be more sensitive than publicly available social media data. Similarly, selling data to a third party may require more oversight than data use tied closely to the function of a product or service, or that is required by law. Finally, data that a company infers or observes about its customers may require different considerations compared to data volunteered by a customer.

Data governance frameworks may also consider the interaction of data types, collection approaches and uses. Companies may choose, for example, to enact strict standards for certain sensitive data types, even if they are volunteered by the customer or used as a core part of a company's business operations. Figure 12 provides an example of a simplified data governance framework; however, in practice, governments and businesses will likely need to tailor their approaches to the opportunities and risks they face in using customer data

Figure 12: Illustrative simplified data governance framework (not prescriptive)



Source: World Economic Forum stakeholder interviews and Oliver Wyman

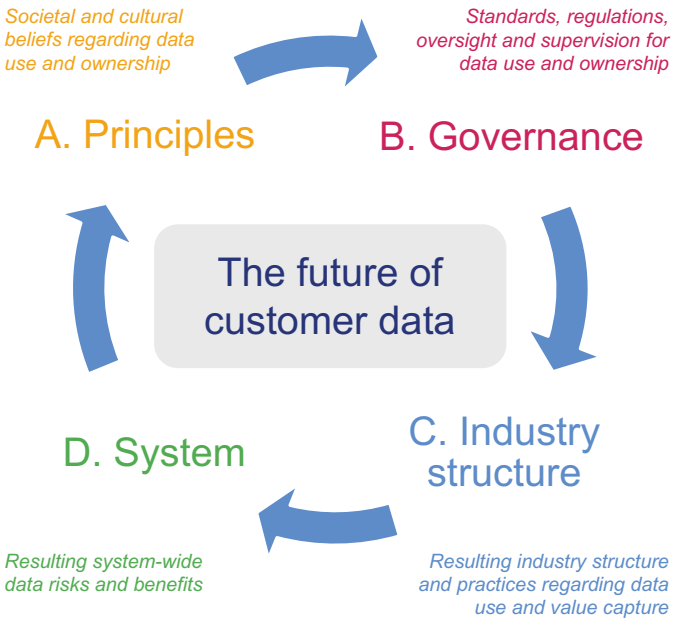
4. Global data principles

The development of global principles for financial services is an important first step in harmonizing customer data laws, regulations and practices. Customer data principles are not a substitute for country- or industry-specific guidance; however, principles can provide a framework (Figure 13) to address the challenges described in the previous sections.

Principles can support coordination across the following dimensions:

- **Regional differences in societal and cultural beliefs.** Europe's focus on data as a human right has emphasized privacy and limited data use. In contrast, Asian countries have stressed the economic benefits of customer data, particularly for financial inclusion. A set of global principles is critical to identifying areas of common ground that balance the opportunities and risks in customer data.
- **Regulatory inconsistencies across jurisdictions.** More than 120 countries around the world have enacted data protection laws. Global principles can provide a useful tool for businesses and governments, particularly in jurisdictions where regulatory frameworks are still being developed in the wake of Europe's GDPR regulation, and where regulatory harmonization is a key consideration.
- **Wide-ranging industry practices and customer experiences.** Companies use different types of data within and across industries in significantly different ways. Global principles can support developing best practices that benefit both businesses and customers.

Figure 13: Customer data framework



Source: World Economic Forum and Oliver Wyman

Principles: *Societal and cultural beliefs are an important arbiter of what are considered fair or unfair uses of customer data. Media attention can also spotlight abuses or highlight innovations that are seen as valuable, even if they are not officially allowed under current regulations.*

Governance: *Characterized by transmission mechanisms for policy-makers and regulators to establish and enforce the rules of the game, this includes standards, regulations, oversight and supervision.*

Industry structure: *Focusing on how data are used in practice and how the value of customer data is distributed, industry structure addresses both customer experience and the relative strengths and weaknesses of incumbents and challengers.*

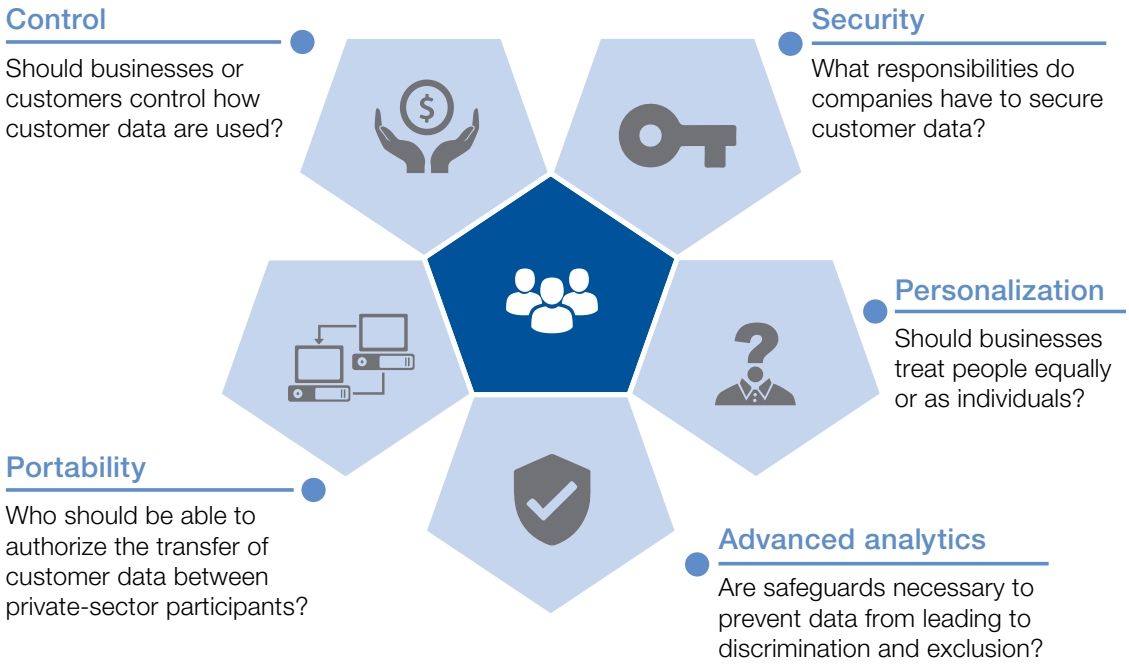
System: *The resulting system-wide opportunities and risks from how data are used will ultimately influence societal and cultural beliefs and restart the cycle.*

> "The economy is reorganizing into a series of distributed peer-to-peer connections across powerful networks – revolutionizing how people consume, work and communicate. The nature of commerce is changing. Sales are increasingly taking place online and over platforms, rather than on the high street. Intangible capital is now more important than physical capital. Data is the new oil. In the financial sector, these innovations will allow people to manage their finances seamlessly, from tracking how much they spend, to managing their future savings and current loans. For the financial sector to be effective in this new economy, it needs to continue to be resilient, fair and dynamic, while acknowledging the responsibilities that come with employing this new data. This is best achieved by combining public regulation with private standards that represent the collective view of best practice and then buttressing them with a series of hard incentives that foster adoption and adherence."

Mark Carney, Chair of Financial Stability Board; Governor of the Bank of England

Customer data principles need to balance the opportunities and risks concerning customer data in financial services. Discussions with the Financial Stability, Innovation and Economic Growth (FSIEG) stakeholders have highlighted the trade-offs associated with the spectrum of five key themes: control, security, personalization, advanced analytics and portability (Figure 14). In each of these areas, focusing too much on customer protection can limit innovation, preventing the development of products and services that create value for customers and businesses. However, data misuse can also pose serious risks, including for customer trust that is needed to support future data-related innovations.

Figure 14: Customer data trade-offs



Source: World Economic Forum and Oliver Wyman

Control balances the relative abilities of businesses and consumers to use and capture value from data. On the business control side of the spectrum, companies would have the right to use any type of customer data for any purpose. This supports innovation but also poses risks of data misuse. With greater customer control, companies need consent to use different types of customer data for a specific purpose. This increases transparency but also creates frictions that can affect the customer experience.

Security balances the opportunities and risks of holding companies responsible for protecting customer data. On the risk side of the spectrum, companies are considered liable for any data breaches. This incentivizes greater investment in cyberprotection but could make it difficult for new entrants to comply with complex regulations. On the opportunity side, customers are ultimately liable for the implications of data breaches. This places the fewest limits on innovation but also requires significant customer due diligence on which companies are most likely to protect data about them.

Personalization balances the benefits of privacy with the advantages of precise customer profiles. On the anonymity side of the spectrum, customers are each offered the same products and services. This enables a high degree of privacy with limited discrimination against protected classes; however, it may weaken profitability, or even lead companies to exit products or markets where the average customer is not profitable. Greater precision allows for more customized profiles for individual customers. This can benefit customers with attractive risk profiles but it can also prevent high-risk customers from gaining access to services.

Advanced analytics balances the opportunities and risks of new models and statistical approaches. Focusing on risk would require companies to limit the use of models that cannot be explained. This can reduce fraud, data inaccuracies or discrimination based on sensitive characteristics; however, it can also restrict innovation, as well as lead companies to avoid entering markets that have limited customer data or where data quality is questioned. On the other hand, focusing on opportunity would mean placing fewer restrictions on model use. This could increase innovation but it could also lead to a higher risk of data misuse or even business failure if companies are not able to employ successful risk management practices.

Portability balances the benefits of open versus closed data ecosystems. In a closed data regime, companies have full control over whether and how to give customers access to data.

This incentivizes curated ecosystems that address a wide range of customer needs but may make switching providers difficult. On the other hand, open data regimes allow customers to download and transfer information, or allow third parties to manage data about them. Open data ecosystems can increase customer choice and reduce switching costs; however, they can also decrease the incentive for companies to invest in their existing data stores.

The Forum-convened stakeholder group has developed a set of global principles for the appropriate use of customer data in financial services. It seeks to balance the trade-offs for each of the five themes. The principles, summarized in Figure 15, are based on interviews and working group meetings with more than 100 stakeholders, including representatives from the Americas, Europe and Asia-Pacific, and from incumbents, fintech companies, governments, academia and law firms. These principles are prioritized according to stakeholder interest and their broad potential for generating trust in the financial services system.

Despite broad consensus on the principles, their implications for customers, governments and businesses were debated. To capture the richness and nuance of these discussions, further details for each of the principles on four important questions are provided, namely:

- What does the principle mean?
- What was the range of perspectives on the principle held by the stakeholder group?
- What conditions are needed for the principle to be effective in practice?
- What factors may affect how the principle is implemented?

Several brief example cases of how companies are thinking about the application of these principles are also included.

Figure 15: Customer data principles

Control

"Companies should be clear about their use of customer data, attain customer agreement to their customer data policies and, where appropriate, seek consent for specific uses."

Key conditions:
- **Informed consent:** Companies need to provide clear and accessible information about how customer data will be used (e.g. terms and conditions).
- **Transparency:** Customers should be able to view or know the data that are collected about them, how they are used and whether they are shared with a third party.
- **Ability to revoke consent:** Customers should be able to request that data about them no longer be used by an organization (e.g. the right to be forgotten).
- **Legitimate use**: Companies may not need to seek consent when using data for legitimate interests (e.g. those required by law).

Security

"Companies should be held responsible and accountable for data security."

Key conditions:
- **Liability:** A clear liability framework should be in place that ensures the responsible party is held accountable for data security and for harms caused by breaches of its respective data security duties of care.
- **Traceability:** Companies need to be able to identify where data were improperly used or accessed in the event of a security breach.

Person-alization

"Companies should be able to create individual customer-level profiles that allow them to provide differentiated customer services."

Key conditions:
- **Intervention:** Customers should be able to intervene to gain information or limit use of data they control, and companies should respond appropriately.
- **Limited use**: Where reasonable, a maximum time period that data can be retained by companies should exist, as well as limits on certain sensitive data types or uses.

Advanced analytics

"Companies should be able to comprehensively test, validate and explain their use of data analytics and models to customers."

Key conditions:
- **Justification:** Customers should have the right to request why a decision was made (e.g. why the model methodology is appropriate, why the output is justified).
- **Challenge:** Customers should have the right to correct incorrect or incomplete data about them held by a company.

Portability

"Companies should, where appropriate, allow customers to access, download, transfer and/or permit third parties to manage data about them."

Key conditions:
- **Accessibility:** Companies should allow customers to download data about them in machine-readable format or through standardized APIs, depending on the companies' stage of development and jurisdiction.
- **Third-party permissions:** Accessibility encompasses customers giving third parties permission to download their data.

Source: World Economic Forum and Oliver Wyman

Control

"Companies should be clear about their use of customer data, attain customer agreement to their customer data policies and, where appropriate, seek consent for specific uses."

What is meant by control?

Control refers to the **relative ability** of businesses and consumers **to use and capture value from data**.

Key questions:

- *When is consent required to use customer data?*
- *What is required for informed consent?*
- *Can customers request to know the data about them held by companies?*

What is the range of perspectives about control?

Most subject matter experts moderately favour **customer control** versus business control over customer data.

Business Control		Range of perspectives	Customer Control
Companies should not need consent to use or share customer data	Companies should need consent to share customer data with third parties	**Companies should need consent to use customer data for different purposes**	Companies should need consent to use different types of customer data for different purposes

What conditions are required to be effective in practice?

- **Informed consent:** Companies need to provide clear and accessible information about how customer data will be used (e.g. terms and conditions).
- **Transparency:** Customers should be able to view or know the data that are collected about them, how they are used and whether they are shared with a third party.
- **Ability to revoke consent:** Customers should be able to request that data about them no longer be used by an organization (e.g. the right to be forgotten).
- **Legitimate use:** Companies may not need to seek consent when using data for legitimate interests (e.g. those required by law).

What factors may affect how control is implemented?

- **Data type:** Identity, financial and health data are seen as requiring stronger customer control than publicly available data (e.g. social media data).
- **Data collection:** Inferred data are viewed as the intellectual property of companies, while customers are seen to retain control over volunteered and observed data.
- **Data use:** Companies should be able to use data for core products and services; however, explicit consent is considered necessary for sharing data with third parties.

Security

"Companies should be held responsible and accountable for data security."

What is meant by security?

Security refers to how **data security responsibility** is balanced between customers and companies.

Key questions:

- *What responsibilities do companies have to secure customer data?*

What is the range of perspectives about security?

Most subject matter experts perceive security as a **risk** rather than an opportunity.

Risk	Range of perspectives		Opportunity
Companies should be considered responsible for data security and liable for any breaches	Companies should follow best practices on data security	Companies should make a reasonable effort to ensure data security beyond legal requirements	Companies should not be considered responsible for data security beyond legal requirements

What conditions are required to be effective in practice?

- **Liability:** A clear liability framework should be in place that ensures the responsible party is held accountable for data security and for harms caused by breaches of its respective data security duties of care.
- **Traceability:** Companies need to be able to identify where data were improperly used or accessed in the event of a security breach.

What factors may affect how security is implemented?

- **Data type:** Certain types of data, particularly identity, financial and health data, are seen as more important to protect compared to anonymized data.
- **Data collection:** This is seen as less relevant, excluding how it may be connected to data type.
- **Data use:** Sharing data may require additional protections, particularly since it involves balancing liability between additional parties.

Personalization

"Companies should be able to create individual customer-level profiles that allow them to provide differentiated customer services."

What is meant by personalization?

Personalization refers to whether companies can provide **differentiated services** to customers.

Key questions:

- *Should businesses treat people equally or as individuals?*
- *To what extent should companies incorporate customer preferences for data use?*

What is the range of perspectives about personalization?

While personalization is actively debated, most subject matter experts lean towards **precision** versus anonymity.

Anonymity		Range of perspectives	Precision
Companies should treat all customers the same	Companies should be able to create broad customer segments	**Companies should be able to create narrow customer segments**	**Companies should be able to create individual customer-level profiles**

What conditions are required to be effective in practice?

- **Intervention:** Customers should be able to intervene to gain information or limit the use of data they control, and companies should respond appropriately.
- **Limited use:** Where reasonable, a maximum time period that data can be retained by companies should exist, as well as limits on certain sensitive data types or uses.

What factors may affect how personalization is implemented?

- **Data type:** Certain types of data may be too sensitive to use – for example, individual characteristics that cannot be changed (e.g. DNA, gender, race).
- **Data collection:** Consent is seen as necessary before using data obtained from third parties.
- **Data use:** Debate continues about whether there should be limitations for specific data uses, or if societal checks should be made on outcomes (e.g. requiring basic provision of services for all customers).

Advanced analytics

"Companies should be able to comprehensively test, validate and explain their use of data analytics and models to customers."

What is meant by advanced analytics?

Advanced analytics refers to whether **safeguards** are needed to use **new models and statistical approaches**.

Key questions:

- *Are safeguards necessary to prevent data from leading to discrimination and exclusion?*
- *Should customers have the right to correct or update data about them?*

What is the range of perspectives about advanced analytics?

While advanced analytics is actively debated, most subject matter experts moderately prefer **risk** to opportunity.

Risk	Range of perspectives		Opportunity
Companies should not be allowed to use models that cannot be explained	**Companies should test and defend the use of models that cannot be explained**	**Companies should comprehensively test models that cannot be explained**	Companies should not face restrictions on the models they use

What conditions are required to be effective in practice?

- **Justification:** Customers should have the right to request why a decision was made (e.g. why the model methodology is appropriate, why the output is justified).
- **Challenge:** Customers should have the right to correct incorrect or incomplete data about them held by a company.

What factors may affect how advanced analytics is implemented?

- **Data type:** Advanced approaches may unintentionally incorporate proxies for sensitive data, such as gender or race, which may be prohibited in certain jurisdictions.
- **Data collection:** Models using large amounts of highly granular observed data could pose privacy concerns.
- **Data use:** Debate continues on whether there should be limitations for specific data uses, or if societal checks should be made on outcomes (e.g. requiring basic provision of services for all customers).

Portability

"Companies should, where appropriate, allow customers to access, download, transfer and/or permit third parties to manage data about them."

What is meant by portability?

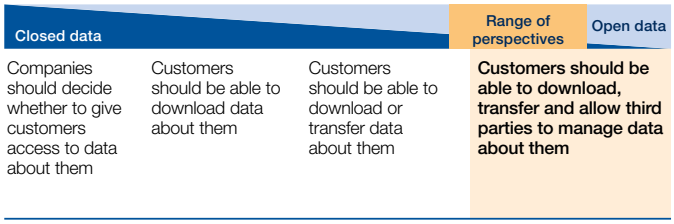
Portability refers to the **ability of customers to transfer data about them** between private-sector participants.

Key questions:

- *Who should be able to authorize the transfer of customer data between private-sector participants?*
- *Do data formatting standards need to be created?*

What is the range of perspectives about portability?

Most subject matter experts lean towards the concept of **open data** versus closed data for portability.



What conditions are required to be effective in practice?

- **Accessibility:** Companies should allow customers to download data about them in machine-readable format or through standardized APIs, depending on the companies' stage of development and jurisdiction.
- **Third-party permissions:** Accessibility encompasses customers giving third parties permission to download their data.

What factors may affect how portability is implemented?

- **Data type:** Identity and demographic data are seen as priorities for data portability, followed by financial data.
- **Data collection:** Inferred data are seen as the intellectual property of companies and should not be portable. While volunteered data provided by the customer should be portable, less consensus exists on observed data.
- **Data use:** Portability is seen as most appropriate for data used for core products and services, or data that are already outsourced to third parties.

Source: World Economic Forum and Oliver Wyman

Example case: Deterring financial crime through data sharing

In a hypothetical case study, fictitious "Mundus Bank" can be used. In this scenario, a Mundus Suspicious Activity Alert is triggered related to an account in Singapore. An investigation is launched, which identifies related trade and transaction flows that include a Singapore account receiving funds via the United Kingdom from Latin America. The payments were for textiles, imported from China to Paraguay. The enquiry also finds that a Mundus account in Dubai sent funds to a second Mundus account in Singapore. The payments were for goods imported to Hong Kong from the United Arab Emirates (UAE). Following the flow of funds, Mundus Bank identifies transactions involving many different jurisdictions. Finally, a parallel investigation is opened by Mundus Turkey that also identifies suspicious activity linked to the Hong Kong account.

In this scenario, Singapore has the most complete view of the potential criminal network, but even there the view is incomplete: data-sharing restrictions in Turkey mean that Singapore has no visibility of Mundus Turkey's investigation. Other jurisdictions have a far less complete view. The UAE will only see the transactions that flow through the UAE account, and Hong Kong's view is similarly restricted. Authorities in Australia, Canada, Mexico, New Zealand, Turkey and the United Kingdom would see nothing. Each Mundus country office must comply with local data-sharing regulations, which prevents Mundus Bank from establishing a complete picture of a client's global footprint. Mundus Bank may not discuss identified financial crime risk in non-Mundus accounts with the banks where additional accounts are held. This hinders it from finding and following critical illicit financial paths in a large network.

Law enforcement and financial institutions have achieved notable successes against illicit finance within individual jurisdictions, despite the considerable barriers to information sharing and collaboration. Increased information sharing would enable banks to better meet the challenge of international illicit finance, while respecting client confidentiality and supporting the growth of international trade.

Rakshit Kapoor, Group Chief Data Officer, HSBC, United Kingdom

Example case: Enabling better customization of product offerings and accelerating underwriting through improved data portability

Data portability in banking provides a complete and almost instantaneous set of customer data in a digital format. It creates a wide range of business opportunities for My Money Bank (MMB), a medium-sized French bank specialized in lending to individuals and SMEs.

Two particular areas stand out:

1. Accelerating the underwriting process by enabling significant process automation and more innovative credit scoring
2. Enabling better customization of product offerings to specific customer contexts and improving cross-selling

Thanks to data portability, MMB will have immediate access to many more customer behavioural indicators (income, spending trends, etc.), in particular through current account statements over a long period of time. Detailed information, i.e. each cash inflow or outflow, is to be clearly identified and classified. Specific behavioural patterns can then be identified from the account activity, leading to new credit scores for the account holder. From these patterns, MMB will gain a much deeper understanding of the customer profile – especially in terms of affordability – and subsequently can provide the customer with a tailored credit proposal.

Accessing customer activity has recently become easier in France thanks to the wider popularity of account aggregation services. Next year, PSD2 (the upcoming European payment directive) will enable financial and non-financial institutions to access the banking activity of retail customers who agree to it. The directive will regulate how the exchange of such data will take place, along preset APIs (interfaces). This will unleash the much wider use of transaction data, beyond the closed realm of the traditional universal banks that hold these accounts.

Three key challenges remain for MMB to achieve such opportunities:

1. Capture and monitor customers' consent over their personal data usage, especially since MMB does not hold customers' primary current bank account
2. Adapt the platform to increase flexibility in quickly connecting to diverse third-party customer data sources
3. Develop more advanced capabilities around data analytics and pattern modelling, i.e. far beyond traditional credit and customer relationship management scorecards

Jean-Pierre Nelissen, Chief Information Officer, My Money Bank, France
Philippe Martinie, Chief Risk Officer, My Money Bank, France

Example case: Underwriting fraud prevention with machine learning

As the price of auto insurance differs from place to place due to risk assessments, people may try to lower their insurance premium by providing false information about their address. This behaviour, however, when the risks are not properly assessed and distributed, results in significant losses for insurance companies and higher prices for customers overall. To cope with these issues, a machine learning solution used in predictive underwriting can support the insurance company by identifying incoming customers at risk of such behaviours in real time. This risk is reflected by a personalized anti-fraud underwriting score. The solution offers controlled levels of fraud, better combined ratios and, in turn, fairer costs for customers.

In cases of automated individual decision-making, including profiling, a privacy impact assessment and the implementation of suitable measures to safeguard the data subject's rights and freedoms (at least the right to obtain human intervention) are important to ensure an adequate level of data protection. In addition, transparency – providing the customer meaningful information about the profiling and its consequences – is essential and promotes customers' trust in new, personalized insurance products.

Philipp Raether, Group Chief Data Protection Officer, Allianz, Germany

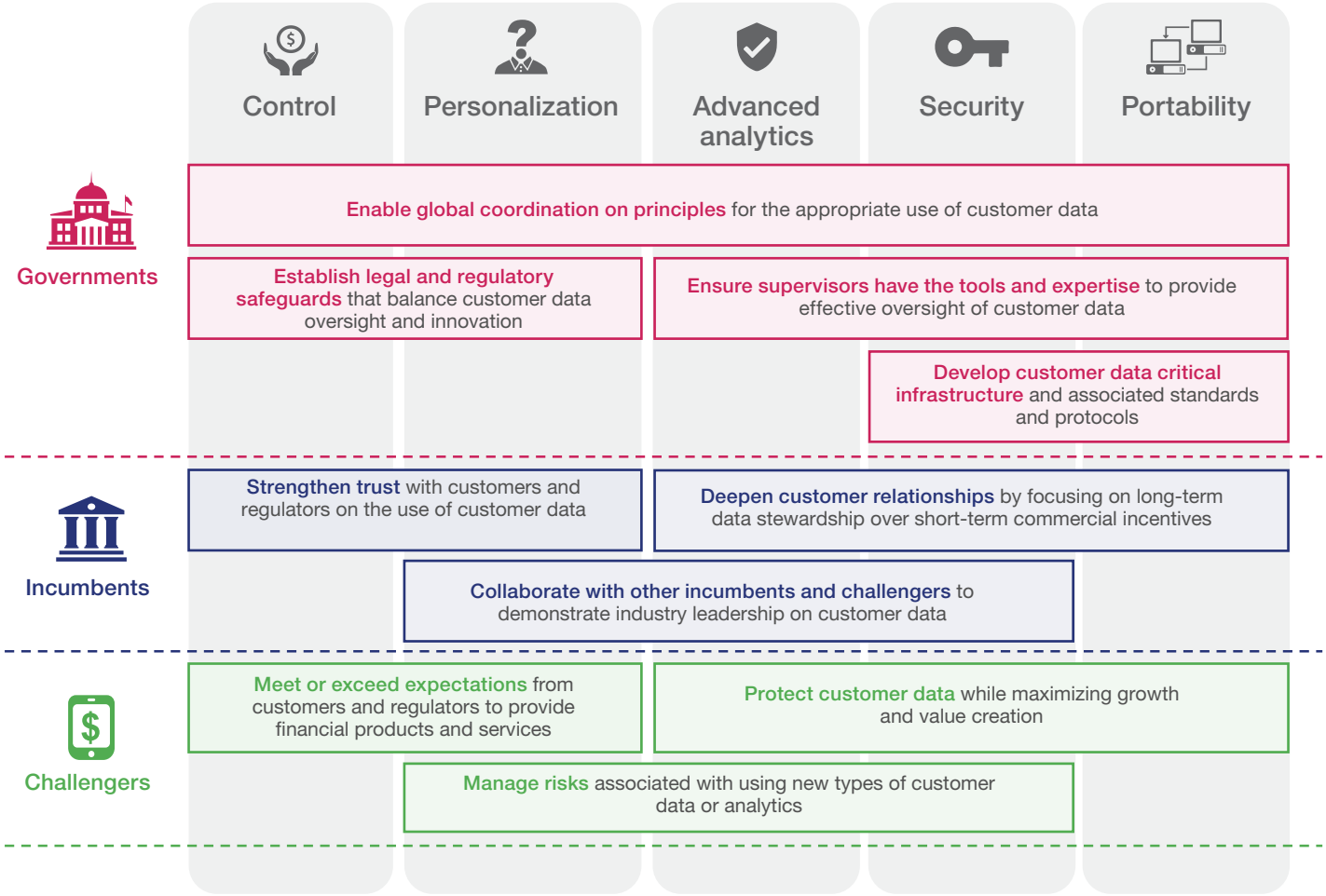
5. Practical government regulation and industry implementation

The principles identified by FSIEG stakeholders demonstrate a relatively high degree of consensus on the appropriate use of customer data in financial services. While stakeholders are still debating several principles, such as personalization and advanced analytics, they provide an important starting point for comparing against existing regulations and industry practices.

The principles suggest a series of next steps for governments, incumbents and challengers faced with practical issues of regulation and implementation. By becoming more aligned with the principles, these stakeholders can better manage the trade-offs of appropriate data use and can address key data-related challenges while maintaining customer trust and economic stability. This alignment is especially important in regions where data frameworks are still under development.

The next steps are organized around key objectives (Figure 16) and examples of action steps for each stakeholder group. Stakeholder interviews and working groups helped to prioritize key objectives for each stakeholder group to take advantage of the opportunities in customer data while mitigating the risks. From there, action steps, which will need to be tailored depending on the region, have been identified for stakeholders to achieve quick wins and thus create a foundation for success. Finally, a brief description is included of the objective's current state, especially related to each region.

Figure 16: Customer data stakeholder objectives



Source: World Economic Forum and Oliver Wyman

The expected effect of GDPR on growth and innovation

A European view on data

Finance has long been an activity built on information, with no physical goods exchanged in most transactions. Unsurprisingly, protecting personal data from fraud or misuse is at the core of banking because it must safeguard customers' financial assets.

The digitization of finance has triggered an evolution towards a true data-driven activity, in which data are not a liability but a source of value for customers. On the one hand, big data analytics is a means to improve processes in the never-ending quest for efficiency, which in turn results in more affordable financial services. On the other, most importantly, data open the door to better understanding customers' true needs and to helping them make better financial decisions.

In Europe, data privacy is considered an individual right that is now reinforced under the GDPR. Critics argue that the GDPR burdens innovation, because it sets such a high standard for data storage, transmission and processing that it increases barriers to entry significantly. Some of the short-term trade-offs in adopting such a demanding regulation are clear. However, achieving economic growth or delivering more innovative solutions to clients should not be at odds with respecting the fundamental right to privacy. The aim must be to achieve both.

We live in a time in which technology enables third parties with access to our data to "discover" our most intimate preferences or beliefs, not to mention our purchase decisions. Privacy is the ultimate guarantee that the ongoing digitization of our lives will still leave individuals in control.

Greater social welfare will be achieved if the right balance is found between protecting individual rights and stimulating friction-free access to and use of data. If the exchange of data for better services is to be a repeating win-win game, it is necessary to ensure that short-term gains do not generate new long-term risks or a general loss of trust between financial intermediaries and their customers.

The GDPR sets a high standard for any company operating in Europe. Though not yet a global standard, it has forced companies and governments around the globe to reflect on the kind of protection individuals deserve. European regulation might be cumbersome in the short term, but it will better prepare firms for a future in which data privacy will be an increasing concern for individuals.

Carlos Torres Vila, Chief Executive Officer, Banco Bilbao Vizcaya Argentaria, Spain

Governments

Objectives	Examples of action steps
1. Enable global coordination on **principles** for the appropriate use of customer data 2. Establish appropriate **legal and regulatory safeguards** that balance customer data oversight and innovation 3. Ensure supervisors have the **tools and expertise** to provide effective oversight of customer data 4. Develop customer data **critical infrastructure** and associated standards and protocols	❑ **Create a customer data bill of rights** defining what companies need to tell customers about how they collect, share and use different types of data (e.g. volunteered, observed, inferred) ❑ **Propose testing guidelines** and a dispute resolution framework for approaches using advanced analytics ❑ **Develop a data liability framework** that ensures the responsible party is held liable for any data breaches ❑ **Develop API standards for open banking** that leverage feedback from industry and align with global practices

Global principles

More than 120 data protection laws exist around the world, with varying objectives and enforcement mechanisms. Given different economic and cultural contexts, data regulations can be expected to differ across countries and regions. However, fragmented regulations, particularly for security, impose significant costs, including organizational inefficiency, uncertainty about jurisdictional oversight and uneven participation in global data flows.

Adopting global customer data principles can help harmonize regulations and support data-fuelled innovation and economic growth. Governments can identify and address regulatory gaps and inconsistencies concerning customer data through common principles. Collaboration and consultation with private-sector participants on principles can make it easier for companies to operate globally and for customers to benefit from cross-border goods and services.

Status: Some convergence has occurred on shared data principles, particularly within Europe. In the United States, the Consumer Financial Protection Bureau has released separate principles focused on consumer-authorized financial data sharing and aggregation. In Asia-Pacific, country-specific principles have been developed in China and Singapore. Further, intergovernmental organizations, such as the Organisation for Economic Co-operation and Development, have issued principles focused on privacy as it relates to customer data.

Next steps: As reflected in meetings with international stakeholders, additional work is needed to develop a more specific understanding of idiosyncrasies related to the use of customer data across regions. This is particularly true for Europe, the Americas and Asia-Pacific as these regions work to develop their own frameworks, and as existing frameworks like the GDPR evolve over time. For emerging markets (e.g. parts of Asia, Africa and the Americas), understanding the costs and benefits of customer data protections will be especially important considering resource limitations and the potential trade-offs regarding economic growth and innovation.

Customer safeguards

Government consumer protection efforts have not kept pace with the growing use of customer data. While consumers have limited awareness of how data about them is used, most believe that providing personal data is part of modern life, and they are willing to share data if they believe there is a fair value exchange. For example, most consumers want companies to use data about them to prevent adverse actions, such as overdraft fees. However, few consumers are willing to allow financial institutions to sell data about them to third parties without additional benefits.

Legal and regulatory safeguards should balance customer data oversight and innovation. This may include focusing on several of the conditions highlighted in the section on principles, including informed consent, transparency, the ability to revoke consent, and legitimate use, which help customers understand and control how data about them is collected, used and shared.

Status: The GDPR has created a comprehensive framework for consumer protection in Europe. In the United States, several federal bills have been proposed following the Facebook congressional hearing, although it is unclear if they will be adopted (note that California has passed state-wide legislation). In Asia-Pacific, some companies have begun to face a customer and regulatory backlash for their data collection and sharing practices; however, most customer protection efforts are in the early stages of development.

Next steps: Governments around the world will need to continue debating and refining approaches to customer safeguards. This could include developing a data "bill of rights" to protect customers, or a data liability framework to ensure responsible parties are held liable for harm caused by data breaches. Additionally, numerous outstanding questions regarding customer protection must be discussed further, such as how stakeholders should approach the distinction between revoking consent for collection of new data and revoking consent for all data ever collected. Lastly, governments will need to continue refining enforcement strategies pertaining to customer data regulations.

Supervisory expertise

Most supervisors have limited experience dealing with customer data. Compared to existing risks, such as market, credit or conduct risk, supervisors may have less knowledge of the underlying technologies related to customer data or of the methodologies used for risk assessment. In addition, the organizational structure of most supervisory bodies is focused on incumbent financial institutions. As new challengers seek to provide financial products and services, supervisors must work with a wider range of firms – from small fintech firms to large technology companies – that may be subject to multiple types of oversight.

New tools and expertise can allow supervisors to provide effective oversight of customer data. Recruitment and training efforts can be expanded, as well as knowledge-sharing efforts within and across regulatory agencies. In addition, governments can also consider using new tools and approaches that leverage public-private partnerships

Status: Regulators around the world have begun to develop new tools and approaches, from regulatory sandboxes to fintech charters. Recruiting new employees, however, is challenging given the limited number of people with relevant skills and the high demand from the private sector.

Next steps: First, additional debate and discussion is needed to clarify the role of financial service regulators in customer data protection. Second, as regulators work to develop new tools and approaches to ensure the appropriate use of customer data, additional work is required to evaluate the respective costs and benefits, as certain regulations may have large effects on costs but few tangible benefits. Finally, effective enforcement may be costly, particularly given limited supervisory resources, which may encourage expanding public-private partnerships.

Critical infrastructure

The financial services system is interconnected and increasingly reliant on data and technology. The benefits of open banking rely on the ability to easily and securely transfer data between companies. Significant logistical and security challenges, however, can complicate sharing data between two banks (or non-bank intermediaries) in the same country, let alone between different countries or different regions. Other essential elements of the financial system also face notable challenges on cybersecurity.

Customer data critical infrastructure can facilitate economic growth and mitigate the risk of catastrophic system failure. Adopting common standards and protocols for open banking or digital identity infrastructure, and leveraging existing world-class standards, such as the Payment Card Industry Security Standards and those of the International Organization for Standardization, can support private-sector innovation on customer data. Incorporating strong cybersecurity practices into protocols can also help address key security challenges, building trust across the financial system.

Status: In Europe, PSD2 has incentivized progress on standards for open banking. However, further work is needed in the United States, where multiple joint ventures between banks, fintech firms and larger technology companies make standardization more difficult. In Asia, technology platforms often offer a range of financial and non-financial services; however, interoperability can be limited and is likely to become a point of focus.

Next steps: Further regulatory guidance may be needed on how data can be shared (e.g. controlled environments, data anonymization guidance). Adopting common standards and protocols for critical infrastructure will likely support private-sector innovation on customer data. One possibility might be to develop API standards for open banking, leveraging industry's feedback and aligning with global practices. Geography will play a key role in the success, however, especially given differences across data policies and in underlying infrastructure between the United States and Asia-Pacific.

Incumbents

Objectives	Examples of action steps
1. **Strengthen trust** with customers and regulators on the use of customer data by proactively addressing data privacy, security and appropriate use 2. **Deepen customer relationships** by focusing on long-term data stewardship over short-term commercial incentives 3. **Collaborate** with other incumbents and challengers to demonstrate industry leadership on customer data	❑ **Develop a customer data strategy** that articulates a clear value proposition on how customer data can create value for customers ❑ **Define "red lines"** for inappropriate uses of customer data, including specific data types, uses and collection approaches ❑ **Establish a dialogue with regulators** to identify industry best practices for appropriate uses of customer data

Customer trust

Incumbents want to better leverage customer data but worry about losing the confidence of customers and regulators. As cited in Figure 6, nearly half of customers would lose trust in their bank if it were accused of unethical business practices that did not affect them personally, and over a quarter would consider switching to a new bank. These survey results highlight the inherent value and fragility of trust as an asset in the financial system, and the possible consequences of its loss. In addition, the cost of regulatory fines is expected to increase. For example, the GDPR allows regulators to penalize a company at up to 4% of its global yearly revenue if data are used inappropriately.

Proactively addressing data privacy, security and the appropriate use of data can strengthen trust. Compared to challengers, incumbents often have long-standing relationships with customers and regulators to serve as a starting point for communicating how they plan to use customer data. Data strategies will vary across institutions. In the future, some institutions may decide to market their reputation for privacy, while others may offer highly-specialized financial products for customers willing to share additional personal data. However, it is critical for all actors to be transparent and highly aware of customer and regulatory concerns.

Status: Trust remains a valuable commodity that may be affected by companies' use of customer data. Compared to challengers, incumbents start with a relatively high level of trust in their use of customer data for financial services.

Next steps: As companies expand their use of customer data, they should remain aware of public perceptions, which can change quickly. Where appropriate, a defined customer data strategy may become useful and could consider efforts to educate customers and improve data literacy.

Data stewardship

Incumbents are facing increasing incentives to commercialize or monetize customer data. In the short term, using such data for marketing purposes, or even selling customer data to third parties, can increase revenue. However, these uses can pose risks to longer-term customer relationships if individuals feel that companies are using data about them to enrich shareholders rather than to create products and services that provide value for customers.

A long-term mindset of data stewardship can deepen customer relationships. Developing a data strategy that clearly articulates appropriate (and inappropriate) uses of data can support a culture where both businesses and customers benefit from the growing use. This culture serves as an important safeguard against the short-term commercial incentives that employees will increasingly face in their day-to-day decisions concerning customer data. To that extent, employees can play a prominent role in a developed data strategy.

Status: Underlying technological capabilities often limit the use of data. Amid additional opportunities to increase revenue through the use of customer data, companies are starting to be mindful of the short- versus long-term value of their existing customer relationships.

Next steps: As systems improve, companies will need to define their own internal governance mechanisms for customer data. These will need to be geographically tailored to customer and regulatory preferences in different jurisdictions. To enhance a culture of data stewardship, companies may also consider offering specialized training for employees on the appropriate use of customer data.

Collaboration

Customer data's complexity challenges incumbents to clearly articulate their customer data strategy to customers and regulators. While incumbents may typically ask for consent to use customer data, some necessary exceptions include deterring terrorism financing or money laundering. Alternatively, for data portability, some limits may be needed on how much data a customer can download or transfer to a third party, accounting for possible proprietary information.

Collaborating more with other incumbents and challengers can demonstrate industry leadership on customer data best practices. By developing a realistic consensus on how principles can be implemented in practice, incumbents can strengthen trust with customers and regulators. Effective self-regulation can reduce the likelihood of costly compliance-focused regulatory efforts. Increased collaboration can also facilitate joint ventures, such as shared data utilities or cybersecurity measures that benefit actors across the financial system.

Status: Incumbents have collaborated on data protection and cybersecurity initiatives, such as Sheltered Harbor in the United States. Significant opportunities exist for incumbents to work together or with challengers to develop best practices on how to use data appropriately; for example, they could leverage prior collaborative work on cyber topics.

Next steps: Incumbents should continue to collaborate to demonstrate industry leadership on customer data and to recognize the many advantages of strengthening trust with customers, reducing the likelihood of compliance-focused efforts and facilitating profitable joint ventures. Challengers can also play a role in collaborating with other industry stakeholders.

Challengers

Objectives	Examples of action steps
1. **Meet or exceed expectations from customers and regulators** to provide financial products and services 2. **Manage risks** associated with using new types of customer data or analytics 3. **Protect customer data** while maximizing growth and value creation	❑ **Enhance terms and conditions and privacy management tools** to provide customers with greater control over how data about them are collected, used and shared ❑ **Develop an appeals process** that provides customers with a rationale for decisions made using advanced analytics and allows them to correct errors in data about them ❑ **Adopt cybersecurity best practices** to build trust and increase opportunities to partner with incumbents

Customer trust

Challengers have both the obstacle and the opportunity of defining a new financial services value proposition for customers. While fintech companies start from a blank slate, larger technology firms face a slightly different challenge of translating their existing reputations on the use of customer data to financial services. Both fintech and large technology firms have an opportunity to convince regulators of the value they can provide to customers while addressing the issue that financial services regulation has not always kept up with technical advances.

Challengers can use their strengths to build trust with customers and regulators. While customers may be hesitant to share data about them with an unknown company, fintech firms can overcome this challenge by clearly communicating how they will use customer data to create innovative products and services. Larger technology firms must clarify whether they will use customer data differently for their financial products and services than for their technology products and services. Finally, both fintech and larger technology firms will need to work with regulators to adapt existing approaches for new financial products and services.

Status: Customers have become more cautious following publicity on recent data breaches but most are still willing to share data about themselves with companies. However, a higher degree of trust is often required for financial data compared with other types of data. Whether established technology companies or relatively new fintech firms can develop this trust will be an important question for the future.

Next steps: Whereas incumbents may need to protect their existing reputations, challengers can start from a relatively blank slate. To develop customer trust, fintech firms may consider developing clear data use policies, enhancing terms and conditions and privacy management tools to provide transparency and greater control to customers on how data about them is collected, used and shared.

Risk management

Challengers are well positioned to develop new products and services leveraging advanced analytics and new forms of customer data. These solutions offer challengers the opportunity to serve new customers outside the traditional financial system, as well as to expand service to customers poorly served by the current system. However, new products and services may also create business risks if companies are unable to effectively manage new risks associated with limitations of alternative data sources or with changing customer risk profiles.

Challengers need enhanced tools and approaches to manage risks and create value. In addition to business risks, challengers should be aware of regulatory risks associated with advanced analytics and alternative data sources, such as unintentional discrimination against protected groups which can also affect customer trust.

Status: A wide range of practices exists on how challengers use data across fintech and large technology companies, as well as across regions. As they evaluate new data sources and models, many firms face challenges in how to collaborate with other firms without giving away valuable intellectual property.

Next steps: Given possible business and regulatory risks, challengers may develop policies targeted to manage these risks and mitigate their effect on customer trust. For example, companies may choose to develop an appeals process that provides customers with a rationale for decisions made using advanced analytics and allows them to correct errors in the data about them.

Data security

Challengers face distinct obstacles in protecting sensitive customer financial data. Smaller fintech firms often have limited resources to devote to cybersecurity, while frequent business model changes can lead them to store larger amounts of customer data that may be useful in the future. Larger technology companies often have greater cybersecurity resources but may have less experience with customer financial data than incumbents.

Customer data security should be considered in the design of new products and services. Data protection by design is both less expensive and less difficult technically than upgrading protections after a data breach. Increased partnerships between incumbents, fintech companies and larger technology firms can also clarify best practices and increase the collective security of the financial services ecosystem.

Status: Efforts are under way to improve data security but more are needed as new firms continue to expand into financial services. The World Economic Forum has recently launched a cyber-consortium including incumbents, fintech firms and large technology companies. The group plans to develop a cybersecurity assessment for fintech firms and data aggregators, building on solutions identified in the Forum's recently published White Paper "Innovation-Driven Cyber-Risk to Customer Data in Financial Services".

Next steps: As new firms expand into financial services, they will need to act to protect financial services data and thus ensure customer trust. Actions may include the adoption of cybersecurity best practices to build trust and increase opportunities to partner with incumbents. Challengers should also consider the data stewardship implications they share with incumbents.

Conclusion

The opportunities for customer data to create value for businesses and customers are enormous. Technology-driven innovation is enabling customized products and services that can better meet customer needs and that allow companies to expand to new markets. However, to fully realize the benefits of customer data, greater consensus is needed across regions and industries on how data should be used appropriately.

The first step is to pursue agreement on a broad set of global principles for the appropriate use of customer data in financial services. The principles identified by the FSIEG stakeholder group in discussions with more than 100 stakeholders – namely, those of control, portability, personalization, advanced analytics and security – offer a way to balance the opportunities and risks in customer data. This balance is critical because too much regulation can stifle innovation, while too little customer protection risks the misuse of data, fraud, cyberattacks and possibly instability from loss of trust in financial institutions.

The stakeholder group has also identified a series of considerations by governments, incumbents and challengers facing the hurdles of practical regulation and implementation. By moving into greater alignment with the principles, these stakeholders can address important challenges, such as how to harmonize customer data regulations, share best practices and strengthen trust with customers. Managing these challenges is essential to take advantage of the opportunities for customer data and, ultimately, to balance financial stability, innovation and economic growth.

References

Accenture, 2016. *Building digital trust: The role of data ethics in the digital age*

Accenture, 2016. *Seizing the Opportunities Unlocked by the EU's Revised Payment Services Directive PSD2: A Catalyst for New Growth Strategies in Payments and Digital Banking*

Allen & Overy, 2018. *Preparing for the General Data Protection Regulation*

Association for Data-driven Marketing and Advertising (ADMA), 2017. *World of Privacy*

Bellman, S.; Johnson, E.; Kobrin, S. and Lohse, G., 2004. "International Differences in Information Privacy Concerns: A Global Survey of Consumers", *The Information Society, Columbia Business School*

Bowcott, O., 2017. "UK counter-terror laws most Orwellian in Europe, says Amnesty", *The Guardian*, 17 January

Cary, C.; Wen, J. and Mahatanankoon, P., 2003. "Data mining: Consumer privacy, ethical policy, and systems development practices", *Human Systems Management*, vol. 22, no. 4, pp. 157-168

CIPP Guide, 2010. "Comparing the Co-Regulatory Model, Comprehensive Laws and the Sectoral Approach"

CitiBank, 2017. *ePrivacy and Data Protection: Who Watches the Watchers? – How Regulation Could Alter The Path of Innovation*, Citi GPS: Global Perspectives & Solutions

Cooper, T. and LaSalle, R., 2016. *Guarding and growing personal data value*, Accenture

Corey, N., 2017. *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Information Technology & Innovation Foundation

DLA Piper, 2017. *Data protection laws of the world: Full handbook*

European Commission, 2015. "Special Eurobarometer 431: Data protection", Survey of European consumers and report

European Union Agency for Fundamental Rights, 2017. GDPR text, information society, privacy and data protection

Forrester, 2016. Oliver Forrester's 2016 Data Privacy Heatmap

Hogan Lovells, 2017. *Asia Pacific Data Protection and Cyber Security Guide 2017: Shifting landscapes across the Asia-Pacific region*

Ivell, T.; Wilkinson, B. and Helps, B., 2017. *Future Proofing Privacy: GDPR Compliance in a Networked Banking System*, Oliver Wyman

Jolly, I., 2017. "Data protection in the United States: overview", Thomson Reuters Practical Law

King, N.J. and Raja, V.T., 2013. "What Do They Really Know About Me in the Cloud? A Comparative Law Perspective on Protecting Privacy and Security of Sensitive Consumer Data", *American Business Law Journal*, vol. 50, issue 2, pp. 413-482

KPMG, 2017. *Crossing the line: Staying on the right side of consumer privacy*

Kshetri, N., 2014. "Big data's impact on privacy, security and consumer welfare", *Telecommunications Policy*, vol. 38, issue 11, pp. 1134-1145

Madden, M. and Rainie, L., 2015. *American's Views About Data Collection and Security*, Pew Research Center

Milberg, S.; Burke, S.; Smith, H. and Kallman, E., 1995. "Values, personal information privacy, and regulatory approaches", Communications of the ACM, vol. 38, issue 12, pp. 65-74

Morey, T.; Forbath, T. and Schoop, A., 2015. "Customer Data: Designing for Transparency and Trust", *Harvard Business Review*, May

Newman, N. "How Big Data Enables Economic Harm to Consumers, Especially to Low-Income and Other Vulnerable Sectors of the Population", adapted from Newman, N., 2014. "The Costs of Lost Privacy: Consumer Harm and Rising Economic Inequality in the Age of Google", *William Mitchell Law Review*, vol. 40, issue 2

Quint, M. and Rogers, D., 2015. *What Is the Future of Data Sharing? Consumer Mindsets and the Power of Brands*, Research report, Columbia Business School and Aimia

Raul, A. (ed.), 2016. *The Privacy, Data Protection and Cybersecurity Law Review, Third Edition*, Law Business Research Ltd

Reinsel, D.; Gantz, J. and Rydning, J., 2017. *Data Age 2025: The Evolution of Data to Life-Critical (Don't Focus on Big Data; Focus on the Data That's Big)*, White Paper, International Data Corporation (IDC)

Rieke, A.; Yu, H.; Robinson, D. and von Hoboken, J., 2016. *Data Brokers in an Open Society*, Upturn/published by Open Society Foundation

United Nations Conference on Trade and Development, 2016. *Data protection regulations and international data flows: Implications for trade and development*

Wintermeyer, L., 2017. "Open banking contagion in the UK", *Forbes*, 7 April

World Economic Forum, 2012. Rethinking Personal Data: *Strengthening Trust*

World Economic Forum, 2016. "Internet Fragmentation: An Overview"

World Economic Forum, 2017. "Balancing Financial Stability, Innovation, and Economic Growth"

Acknowledgements

Stewards of the System Initiative on Shaping the Future of Financial and Monetary Systems

The project team offers its special gratitude to the Stewards of the System Initiative on Shaping the Future of Financial and Monetary Systems for their oversight of the Balancing Financial Stability, Innovation and Economic Growth initiative.

Stewards

Oliver Bäte, Chief Executive Officer, Allianz, Germany
Eric Jing, Chief Executive Officer, Ant Financial Services Group, People's Republic of China
Carlos Torres Vila, Chief Executive Officer, Banco Bilbao Vizcaya Argentaria (BBVA), Spain
Ana Botín, Group Executive Chairman, Banco Santander, Spain
Brian T. Moynihan, Chairman and Chief Executive Officer, Bank of America Corporation, USA
Stephen S. Poloz, Governor of the Bank of Canada
Mark Carney, Governor of the Bank of England
Haruhiko Kuroda, Governor of the Bank of Japan
Laurence D. Fink, Chairman and Chief Executive Officer, BlackRock, USA
Patrick Njoroge, Governor of the Central Bank of Kenya
Elvira Nabiullina, Governor of the Central Bank of the Russian Federation
Mauricio Cardenas, Minister of Finance and Public Credit of Colombia
Tidjane Thiam, Chief Executive Officer, Credit Suisse, Switzerland
Michael C. Bodson, President and Chief Executive Officer, Depository Trust & Clearing Corporation (DTCC), USA
John Flint, Chief Executive Officer, HSBC Holdings, United Kingdom
Ralph Hamers, Chief Executive Officer, ING Group, Netherlands
Liu Mingkang, BCT Distinguished Research Fellow, Institute of Global Economics and Finance, Chinese University of Hong Kong, Hong Kong SAR
David Lipton, First Deputy Managing Director, International Monetary Fund (IMF), Washington DC
Daniel Glaser, President and Chief Executive Officer, Marsh & McLennan Companies, USA
Ajay S. Banga, President and Chief Executive Officer, Mastercard, USA
José Antonio González Anaya, Secretary of Finance and Public Credit of Mexico
John Rwangombwa, Governor of the National Bank of Rwanda
Min Zhu, Chairman, National Institute of Financial Research, People's Republic of China
Dan Schulman, President and Chief Executive Officer, PayPal, USA
José Viñals, Chairman, Standard Chartered Bank, United Kingdom
Makoto Takashima, President and Chief Executive Officer, Sumitomo Mitsui Banking Corporation, Japan
Axel A. Weber, Chairman of the Board of Directors, UBS, Switzerland
H.M. Queen Máxima of the Netherlands, United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA), New York
Alfred F. Kelly, Chief Executive Officer, Visa, USA
Joaquim Levy, Chief Financial Officer, World Bank Group, Washington DC

Steering Committee

The project team thanks the members of the multistakeholder Steering Committee for their leadership of the Balancing Financial Stability, Innovation and Economic Growth initiative.

Members

Stefano Aversa, Global Vice-Chairman and Chairman, Europe, Middle East and Africa, AlixPartners, United Kingdom
Sanjiv Bajaj, Managing Director, Bajaj Finserv, India
Thong Nguyen, President, Retail Banking; Co-Head, Consumer Banking, Bank of America, USA
Kevin Lynch, Vice-Chairman, BMO Financial Group, Canada
Barbara Novick, Vice-Chairman, BlackRock, USA
Bertrand Badré, Chief Executive Officer, BlueOrange Capital, USA
Ashish Gupta, President, United Kingdom; President, Global Banking and Financial Services, BT, United Kingdom
Elvira Nabiullina, Governor of the Central Bank of the Russian Federation
Malcolm Sweeting, Senior Partner, Clifford Chance, United Kingdom
Benoît Coeuré, Member of the Executive Board, European Central Bank, Frankfurt

Domingo Sugranyes Bickel, Chairman, Fondazione Centesimus Annus Pro Pontifice, Vatican City State
Matthew Gamser, Chief Executive Officer, Small and Medium Enterprise Finance Forum, International Finance Corporation (IFC), Washington DC
Paul Andrews, Secretary-General, International Organization of Securities Commissions (IOSCO), Australia
Richard Eldridge, Chief Executive Officer, Lenddo, Singapore
Jeff Stewart, Founder and Chairman, Lenddo, Hong Kong SAR
Erik Berglöf, Professor and Director, Institute for Global Affairs, London School of Economics and Political Science, United Kingdom
Kush Saxena, Chief Technology Officer, Markets and Transformation, Mastercard, USA
Alain Demarolle, Chairman, My Money Bank, France
Greg Medcraft, Director, Organisation for Economic Co-operation and Development (OECD), Paris
Jonathan Auerbach, Executive Vice-President, Chief Strategy and Growth Officer, PayPal, USA
David McKay, President and Chief Executive Officer, RBC (Royal Bank of Canada), Canada
Mark Hawkins, President and Chief Financial Officer, Salesforce.com, USA
Masahiko Oshima, Director, Member of the Board and Senior Managing Executive Officer, Sumitomo Mitsui Banking Corporation, Japan
Cecilia Skingsley, Deputy Governor of the Swedish Central Bank (Sveriges Riksbank), Sweden
Thomas Moser, Alternate Member of the Governing Board, Swiss National Bank, Switzerland
Eric Duflos, Director, United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA), New York
Michael Budolfsen, President, UNI Europa Finance, UNI Global Union, Switzerland
Randall Kroszner, Norman R. Bobins Professor of Economics, University of Chicago, USA
Ellen Richey, Vice-Chairman and Chief Risk Officer, Visa, USA
Kapil Wadhawan, Chairman, Wadhawan Group, India
Cahit Erdogan, Head, ITC and Operations, Yapi Kredi Bank, Turkey

Data Working Group

The project team also thanks the Data Working Group for its contributions to the Balancing Financial Stability, Innovation and Economic Growth initiative.

Members

Au Chong Wai, Deputy Group Head Legal, AirAsia, Malaysia
Tao Sun, Senior Economist, Ant Financial Services Group, People's Republic of China
Long Chen, President, Alibaba Digital Economy Institute, People's Republic of China
Rosie Thomas, Executive Officer, Australian Securities and Investment Commission (ASIC), Australia
Chloe Youl, Senior Manager, Australian Securities and Investment Commission (ASIC) Australia
Neil Munroe, President, Management Board, Association of Consumer Credit Information Suppliers, Belgium
Rakesh Bhatt, Chief Operating Officer, Bajaj Finance, India
Alvaro Martin Enriquez, Lead Economist, Banco Bilbao Vizcaya Argentaria (BBVA), Hong Kong SAR
Cristina San José Brosa, Chief Data Strategist, Banco Santander, Spain
Ezequiel Szafir, Chief Executive Officer, Openbank, Banco Santander, Spain
Jim Catlin, Analytics and Information Executive, Bank of America, USA
Darcy Bowman, Senior Legal Counsel, Bank of Canada, Canada
David Wu, Chief Strategy Officer, Business Big Data, People's Republic of China
Kaitlin Asrow, Manager, Center for Financial Services Innovation, USA
Beth Brockland, Director, Center for Financial Services Innovation, USA
Konstantin Trusevich, Consultant, Department of Financial Technology, Central Bank of the Russian Federation, Russian Federation
Olivier Crespin, Senior Managing Director, Chief Fintech Officer, CIMB Group Holdings, Malaysia
Andres Wolberg-Stok, Global Head of Policy, Citi FinTech, Citi, USA
Paul Landless, Partner, Clifford Chance, Singapore
Lamberto Barbieri, Managing Director, Asia, CRIF, Singapore
Luisa Monti, Director, Regulatory Developments and Innovation Support, CRIF, France
Corey Stone, Senior Advisor, Consumer Financial Protection Bureau, USA
Malte Beyer-Katzenberger, Policy Officer, European Commission/Eurostat, Luxembourg
Tony Hadley, Senior Vice-President, Government Affairs and Public Policy, Experian, USA
Robert Tann, Investment Specialist, Financial Sector, Fondazione Centesimus Annus Pro Pontifice, Vatican City State

Timothy Morey, Vice-President, Innovation Strategy, frog design, USA
Richard Tyson, Principal Strategy Director, Gensler, USA
Simon Burns, Partner, TMT, Gilbert & Tobin, Australia
Michel Cueilhes, Head, Risk and Compliance, GrabPay, Singapore
Rakshit Kapoor, Group Chief Data Officer, HSBC, United Kingdom
Rebecca McCaughrin, Senior Economist, Global Markets, International Monetary Fund (IMF), Washington DC
Sam Taussig, Head, Global Policy and Community Banking, Kabbage, USA
Jaxon Klein, Chief Executive Officer, Co-Founder, Keyo, United Kingdom
Scott Farrell, Partner, King & Wood Mallesons, Australia
JoAnn Stonier, Chief Data Officer, Mastercard, USA
Erika Brown Lee, Senior Vice-President and Assistant General Counsel, Mastercard, USA
Jean Pierre Nelissen, Chief Information Officer, My Money Bank, France
Pranav Seth, Head, E-Business, Business Transformation and Fintech, Oversea-Chinese Banking Corp. (OCBC), Singapore
Richard Nash, Vice-President, Global Government Relations, PayPal, USA
Tyler Spalding, Senior Manager, Corporate Affairs, PayPal, USA
Kevin Moss, Chief Risk Officer, Social Finance US, USA
Suzan Van De Kerk, Head of Operations, APAC, Swiss Re, Singapore
Christophe Tummers, Managing Director and Head, Data and Analytics, UBS, Switzerland
Thomas Pohl, Managing Director, Group Governmental Affairs, UBS, Switzerland
Jayasri Priyalal, Regional Director, UNI Apro Finance, UNI Global Union, Singapore
Rachel Botsman, Visiting Academic and Lecturer, Said Business School, University of Oxford, United Kingdom
Scott David, Director, Policy, Center for Information Assurance and Cybersecurity, University of Washington, USA
David Symington, Policy Specialist, Office of the United Nations Secretary-General's Special Advocate for Inclusive Finance for Development (UNSGSA), New York
Todd Fox, Vice-President, Global Government Relations, Visa, USA
Theodore Waddelow, Director, Strategy and Operations, Global Government Relations, Visa, USA
Bora Uzum, Head, Data Governance, Yapi Kredi Bank, Turkey

Project Team

The development of this White Paper was supported by the project team:

Members

Matthew Blake, Head of the System Initiative on Shaping the Future of Financial and Monetary Systems, Member of the Executive Committee, World Economic Forum LLC
Kai Keller, Project Lead, Balancing Financial Stability, Innovation and Economic Growth Initiative, World Economic Forum LLC
Ted Moynihan, Managing Partner and Global Head, Financial Services, Oliver Wyman (MMC), United Kingdom
Douglas Elliott, Partner, Financial Services, Oliver Wyman (MMC), USA
Alina Lantsberg, Partner, Financial Services, Oliver Wyman (MMC), USA
Alison Flint, Associate, Financial Services, Oliver Wyman (MMC), USA
Ryan Singel, Associate, Financial Services, Oliver Wyman (MMC), USA

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org