OLIVER WYMAN

DATA RIGHTS IN FINANCE: KEY PUBLIC POLICY QUESTIONS AND ANSWERS

AUTHOR
Douglas J. Elliott, Partner
douglas.elliott@oliverwyman.com

DATA RIGHTS IN FINANCE: KEY PUBLIC POLICY QUESTIONS AND ANSWERS

Financial sector policymakers are increasingly focused on data rights, touching on such questions as: who owns financial data, what rights do various parties have to use that data and in which ways, and what privacy rights do individuals have.

These issues are complex and many of them relatively new to policymakers in the financial sector. This primer is intended to explain the key issues and options for policymakers by answering a series of questions:

- Why should financial policymakers care about data rights?
- Why consider financial data separately from other types of data?
- What is financial data?
- How should we think about data ownership, usage rights, and privacy?
- What are the objectives of financial data policy?
- What decisions do policymakers need to make?
- What is the role of "informed consent"?
- What are the key trade-offs?
- What is "open banking"?
- What proposed principles or standards exist?
- How should data rights be regulated?
- What have countries and regions done to date?

WHY SHOULD FINANCIAL POLICYMAKERS CARE ABOUT DATA RIGHTS?

A rich and deep pool of data is increasingly important to decision making in the financial sector, for lending decisions, advice to individuals on investments, algorithmic trading, marketing, risk management, and many other purposes. Governor Mark Carney of the Bank of England has described data as "the new oil". This oil fuels potentially dramatic increases in the efficiency and effectiveness with which businesses can provide financial services, expands financial access by providing alternatives to traditional data sources, and potentially widens the range of services offered.

At the same time, there have been a series of major scandals involving data, usually either relating to the perceived misuse of data for nefarious or unauthorized purposes or stemming from a data breach. These scandals have strongly increased public consciousness of data issues and the level of concern about data protection for individuals. This new focus spurred legislation such as Europe's General Data Protection Regulation and new or proposed laws in a number of other jurisdictions, including the California Consumer Privacy Act (CCPA).

Beyond compliance issues, firms may well feel a broader fiduciary duty towards their customers as regards data, regardless of whether laws or regulations create a formal fiduciary obligation. Companies that view customers as important stakeholders will wish to treat them fairly and to keep their data safe.

Policymakers must determine how best to balance important and somewhat conflicting objectives, to take advantage of the benefits new data sources and analytical approaches offer for society while ensuring appropriate protection of individual data privacy and other rights. This is described in greater detail below.

WHY CONSIDER FINANCIAL DATA SEPARATELY FROM OTHER TYPES OF DATA?

This primer focuses on financial data, but why should policymakers consider this separately from all other types of data? First, it will be possible in many countries to move faster in this sector than more broadly across society, in part because there are regulators specifically focused on the financial sector and in part because it raises a narrower set of issues. Second, financial data is often particularly sensitive and therefore benefits from a specific focus. Third, banks, insurers, and some other types of financial services providers have a considerably greater need for historical data on an individual than do most other business sectors. (Decisions about loans and insurance depend heavily on information about past circumstances and behaviors.) Fourth, waiting for decisions to be made by society about general data rules may mean that those rules are ill-designed for some of the special characteristics of the financial sector.

That all said, clearly financial data is only one piece of the larger puzzle and it will be important that financial policymakers take account of changes in the broader data rights frameworks and that they engage in a dialogue with those seeking to create or change that broader framework.

WHAT IS FINANCIAL DATA?

There remains the question as to where to draw the perimeter around “financial data”. It is impossible to avoid gray areas, but the core concept is that it encompasses data that is used by financial institutions or other firms or individuals to conduct financial services business, whether lending, payments, investments, or other such activities. Note that data does not cease to be financial in nature simply because a business that is not a financial institution is using it in connection with the offering of a financial service.

Another gray area arises when non-financial data is used in financial decisions, such as affiliations that are picked up through social media, like membership in a golf club, that may influence lending.

HOW SHOULD WE THINK ABOUT DATA OWNERSHIP, USAGE RIGHTS, AND PRIVACY?

There are three overlapping frameworks for data rights that policymakers will need to consider. First, some speak of “ownership” of data, with particular emphasis on data about individuals, in which case ownership is generally vested in that individual. Second, others focus on “usage rights”. Thirdly, “data privacy” is often viewed as the central issue. These are not mutually exclusive, as there could be an owner of the data while others might still have usage rights, either automatic or granted by the owner, and data privacy overlaps with both concepts.

The distinctions and overlaps may be better understood by taking the analogy of land. Most legal systems, and languages, recognize the concept of an owner of a piece of land. At the same time, legal systems usually deny landowners certain kinds of usage rights or grant them to others. For example, a landowner generally is not allowed to pollute the land and zoning restrictions may keep them from building large structures or conducting certain types of activities, such as having a store operate out of a building zoned "residential." Further, neighboring landowners may have the right to a portion of the water that flows into a piece of land and the public may have the right to cross a piece of land on a hiking trail that has existed for years.

The distinction between usage rights and ownership takes on even more significance with data, since it:

- Can be in the possession of tens or even thousands of parties at the same time with minimal loss of marginal value to any one possessor
- Can be created in multiple different ways, ranging from a statement of the relevant individual to inferences drawn from other data
- Can be used simultaneously in a multitude of different ways

Data privacy is another overlapping concept. It implies the ability of an individual to grant or curtail certain usage rights to others, or even for these rights to be automatically curtailed by a legal requirement for only the minimal necessary data to be collected or a requirement to delete data after a certain period.

Which framework a policymaker uses for their main focus will affect the choices they are likely to make. As noted, for example, framing the discussion in terms of "ownership" will tend to increase the emphasis on data privacy, with the individual as the owner, potentially at the expense of other objectives.

WHAT ARE THE OBJECTIVES OF FINANCIAL DATA POLICY?

Policymakers strive to achieve multiple varied—and sometimes conflicting—objectives, based on the diverse stakeholders involved in the financial industry. To start, policymakers must consider the following consumer interests:

- **Data sovereignty:** empowering consumers to maintain appropriate control over data about their identity, choices, activities, and situation, including understanding the intentions of the companies that have data about them
- **Data security:** promoting a system in which the risk of unauthorized access to consumer data is minimized
- **Accuracy and appropriate use:** mandating that companies maintain correct consumer data records and use data carefully to make decisions about individuals, such as avoiding inappropriate outcomes from "black box" analytical techniques
- **Financial access:** promoting access to the financial system, through reductions in product costs or other barriers to access

Policymakers must also consider the business community when crafting data governance policy. Objectives central to policymakers' thinking in this respect are:

- **Responsible innovation:** promoting an environment in which businesses are both incentivized and enabled to develop new financial products, including more personalized products, and better ways of offering existing products
- **Competition:** shaping markets that provide ample opportunity for new business entry, to improve total welfare
- **Efficiency and effectiveness:** enabling businesses to operate effectively without regulatory burdens or other costs that go beyond what is necessary
- **Level playing field:** developing policy that minimizes differences in how regulatory requirements apply to business entities subject to different forms of oversight

Finally, policymakers must incorporate certain "general good" objectives into policy, which, though lacking a definitive constituency, are nevertheless essential to the long-term health of the financial system. These objectives include:

- **Financial Stability:** maintaining a strong and resilient financial system
- **Clarity:** advancing a regulatory framework that provides clear guidance and well-defined expectations to firms and consumers, especially with respect to accountability for data throughout its lifecycle
- **Harmonization:** coordinating appropriately with other laws and regulations, including outside the financial sector and beyond jurisdictional boundaries

WHAT DECISIONS DO POLICYMAKERS NEED TO MAKE?

Policymakers ultimately face a long list of decisions they will need to make regarding financial data rights, including:

- How should financial policymakers coordinate with larger national data policy agendas?
  - How should financial data rights fit within human or societal rights associated with data in and across jurisdictions?
  - What broader data rights, constraints or strictures need to be navigated?
  - Where should financial policymakers seek to change or clarify such rights or constraints?
- What are the overall objectives and how are they prioritized?
- Should the focus be on data ownership or on usage rights or a combination?
- What is the role of "informed consent"?
- How should privacy rights be protected? What other rights will individuals have?
- What counts as "financial data"?
- What data dimensions are important for setting policy?
  - Source of data (declared, observed, inferred)
  - Type of consent obtained, if any
  - Level of sensitivity of data
  - Ability to identify individuals
  - Age and accuracy of data
  - Frequency of use

- How should different uses be considered?
  - Internal vs. marketing vs. transfer/sale
  - Product or service involved
  - Used for firm to make a decision vs. to help an individual make a decision
- Should different types of businesses be treated differently?
  - Bank or other financial institution
  - Fintech
  - Big Tech
  - Small business versus large
  - Other
- How should data be protected and by whom?
- How should data rights be governed? Should there be a separate authority?
- What governance processes will be required within businesses?
- How should data issues be coordinated internationally? To what extent is "data localization" needed? What metrics or target outcomes should be established?

WHAT IS THE ROLE OF "INFORMED CONSENT"?

There is a broad policy consensus that certain data about an individual should not be used by a business without the consent of that individual. Further, that consent should be "informed" by appropriate knowledge. The difficulty is in applying this in practice.

There is the threshold question of which data items should require such consent, but the questions do not stop there. They include:

- Can consent be implied by other actions, or must it be explicit?
- Is it reasonable to gain consent for a very broad category of data with one assent, or must there be more specificity?
- What information is necessary for an individual to be considered informed?
- To what extent does this vary by the type of individual or data or usage?
- Is it acceptable to have the information available on request or must it be prominently displayed?
- How legalistic can the consent process be?
- Are there situations in which consent may be considered coerced, such as if it necessary for the use of a product or service that is indispensable or nearly so?

WHAT IS "OPEN BANKING"?

A number of countries have adopted, or are seriously considering, some form of "open banking" requirement. The core idea is that consumers should have the right to authorize third parties to access their financial data from a bank through an API (application program interface). The third party would most often be a fintech (financial technology firm), another bank, or another financial services provider. That third party would use the data to enable the offering of one or more financial services to the consumer.

A crucial motivation for policymakers to institute open banking is the desire to allow consumers more control of their data and of their financial lives. In some countries, there is also explicitly the intent to foster greater competition in banking sectors that are perceived to be oligopolistic. There may also be a desire to encourage the development of fintechs in order to modernize a financial system or to make a financial center in that nation more attractive and effective.

There are a number of questions to be answered if policymakers wish to institute open banking, including:

- What data should be made available?
- To what extent does this include data developed by a bank using internal algorithms?
- Should the bank be able to charge the third party or individual for providing the data?
- What must a third party do to qualify for access, particularly in regard to cybersecurity?
- Who is responsible and what are the penalties if there is a data breach?
- Is there any element of reciprocity, whereby the third party has to provide data to the bank in return?

Several countries have already implemented some form of open banking and a number of others are considering doing so. The UK began implementing open banking in January 2018 through a staged roll-out, beginning with data on the most straightforward financial products. The European Union created a regulation known as PSD 2 that, among other things, requires the largest banks to move to open banking, with national implementation occurring on timetables determined by each country, but generally starting in the near future. Australia has also chosen to implement open banking, with a requirement for phased implementation beginning in July 2019. Readers desiring more details can refer to pages 16 to 19 of Canada's consultation document from the Department of Finance on "A Review into the Merits of Open Banking," published in January 2019 and available at https://www.fin.gc.ca/activty/consult/2019/ob-bo/pdf/obbo-report-rapport-eng.pdf.

WHAT ARE THE KEY TRADE-OFFS?

Optimal policies can minimize, but generally not eliminate, the following trade-offs, among others:

Data privacy and individual control versus efficiency and effectiveness. Individual privacy and control of data are most thoroughly protected when there are automatic restraints on the use of data by businesses (such as requirements for data minimization and for the deletion of older data) coupled with individual rights to determine what data businesses have and keep and how they can use that data. On the other hand, businesses can generally provide the cheapest, best, and widest range of services that rely on financial data if they face minimal restraints from data privacy requirements. Finding the right balance between these interests is one of the most important choices for policymakers.

Data privacy and individual control versus financial inclusion. Tight constraints on use of data can make it harder for businesses to determine which individuals are acceptable risks for loans, insurance, or other services. In some cases, these individuals would not be deemed acceptable risks using more limited and conventional data sources. Extensive use of data may also allow cheaper operations that make some services affordable to individuals who would otherwise be excluded from the financial system as a practical matter. However, policymakers will have to weigh this against privacy rights and data control for consumers.

Portability versus cybersecurity. Policymakers may desire to enhance data portability either as an individual right or in the hopes of increasing competition in the financial sector. However, greater movement of sensitive financial data about individuals increases the risk of a data breach, all else equal.

Data localization versus efficiency and effectiveness. Some national policymakers desire to keep data about their residents stored inside the country. This could be because they view their data rights regime or cybersecurity as superior or could be a matter of industrial policy. At the same time, this increases the cost for businesses that operate across borders and can lessen the effectiveness of anti-money laundering and other operations that benefit from global information.

National standards versus efficiency and effectiveness. Similarly, differing national standards for data rights allows national authorities to match the requirements to their objectives. However, it also adds to costs and decreases the effectiveness of business activities.

Efficiency and effectiveness versus assurance of competition. In at least some cases, firms may be willing to devote more effort and investment into products that rely on heavy use of financial data if they can retain the competitive advantage of doing so (somewhat like patent protection.) However, allowing such data siloing may reduce competitive pressures. One example of this is the tension between data portability and the value to a business of developing processes dependent on that data. Depending on the extent to which data must be shared, it may allow a firm's processes to be reverse engineered, reducing the value to the innovator by introducing further competition.

WHAT PROPOSED PRINCIPLES OR STANDARDS EXIST?

Although we remain far from having agreement on global standards for data rights, let alone common regulations or legislation, there have been a number of proposals for principles that could be adopted globally that would underlie national, and perhaps eventually global, regulatory and legal approaches. A summary of some of the most significant sets of principles is shown below. Please note that in many cases there is considerably more detail supporting these principles, which can be found in the original documents footnoted here.

OECD (Organization for Economic Co-operation and Development) Privacy Principles, 1980[1]

Adopted in the early stages of the "Information Society", these principles provide the foundation for much of the thinking about data governance today.

1. **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the

[1] Source: http://oecdprivacy.org/. Introduction is our own commentary; principle headings and descriptions are directly quoted from the OECD source document.

fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the preceding paragraph] except: (a) with the consent of the data subject; or (b) by the authority of law.
5. **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle:** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him: (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to him; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

CFPB (Consumer Financial Protection Bureau, US) Consumer Protection Principles, 2017[2]

The CFPB Principles build on the OECD's, however they place greater emphasis on financial data and data sharing.

1. **Access:** consumers can request information about the data that data controllers possess about them. Accessing financial products or services does not require consumers to share information with third parties.
2. **Data Scope and Usability:** consumers can authorize data controllers to share their financial data with third parties; this information must be in a format that is "readily usable". Authorized third parties can only access data necessary to provide the consumer's selected products/services and for a limited time.
3. **Control and Informed Consent:** terms of access, storage, use, and disposal are clearly communicated to the consumer and are not overly broad. Consumers are not coerced into granting third-party access and can easily revoke access.
4. **Authorizing Payments:** authorized data access is not by itself payment authorization; this requires distinct consumer authorization.
5. **Security:** data is stored securely and in a format that mitigates breaches. Third parties accessing consumer data meet the same security standards.
6. **Access Transparency:** consumers can readily ascertain complete information about the third parties they have authorized to access their data.

[2] Source: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf. Introduction is our own commentary; principle headings are directly quoted from the CFPB source document; the descriptions are adapted from the CFPB source document, for brevity and clarity.

7. **Accuracy:** consumers can expect data to be accurate and current and can readily dispute and resolve data inaccuracies.
8. **Ability to Dispute Unauthorized Access:** consumers can dispute data access they deem to be unauthorized; such unauthorized entities are held accountable.
9. **Efficient and Effective Accountability Mechanisms:** commercial participants are accountable for data misuse and are incentivized to prevent such activity.

Google Framework for Responsible Data Protection Regulation, 2018[3]

In response to growing public concern about technology companies, Google produced a set of data protection recommendations. These principles provide a perspective from one of the world's largest data holders.

Requirements

- Collect and use personal information responsibly
- Mandate transparency and help individuals be informed
- Place reasonable limitations on the manner and means of collecting, using, and disclosing personal information
- Maintain the quality of personal information
- Make it practical for individuals to control the use of personal information
- Give individuals the ability to access, correct, delete, and download personal information about them
- Include requirements [for organizations] to secure personal information

Scope and Accountability

- Hold organizations accountable for compliance
- Focus on risk of harm to individuals and communities
- Distinguish direct consumer services from enterprise services
- Define personal information flexibly to ensure proper incentives and handling
- Apply the rules to all organizations that process personal information
- Design regulations to improve the ecosystem and accommodate changes in technology and norms
- Apply geographic scope that accords with international norms
- Encourage global interoperability

[3] Source:
https://services.google.com/fh/files/blogs/google_framework_responsible_data_protection_regulation.pdf
Introduction is our own commentary; principles are directly quoted from Google source materials.

NTIA (National Telecommunications and Information Agency, an agency of the US Commerce Department) Consumer Privacy Principles, 2018[4]

The NTIA has released a set of privacy principles for feedback from stakeholders.

1. **Transparency:** Users should be able to easily understand how an organization collects, stores, uses, and shares their personal information. Transparency can be enabled through various means. Organizations should take into account how the average user interacts with a product or service, and maximize the intuitiveness of how it conveys information to users. In many cases, lengthy notices describing a company's privacy program at a consumer's initial point of interaction with a product or service do not lead to adequate understanding. Organizations should use approaches that move beyond this paradigm when appropriate.
2. **Control:** Users should be able to exercise reasonable control over the collection, use, storage, and disclosure of the personal information they provide to organizations. However, which controls to offer, when to offer them, and how they are offered should depend on context, taking into consideration factors such as a user's expectations and the sensitivity of the information. The controls available to users should be developed with intuitiveness of use, affordability, and accessibility in mind, and should be made available in ways that allow users to exercise informed decision-making. In addition, controls used to withdraw the consent of, or to limit activity previously permitted by, a consumer should be as readily accessible and usable as the controls used to permit the activity.
3. **Reasonable Minimization:** Data collection, storage length, use, and sharing by organizations should be minimized in a manner and to an extent that is reasonable and appropriate to the context and risk of privacy harm. Other means of reducing the risk of privacy harm (e.g., additional security safeguards or privacy enhancing techniques) can help to reduce the need for such minimization.
4. **Security:** Organizations that collect, store, use, or share personal information should employ security safeguards to secure these data. Users should be able to expect that their data are protected from loss and unauthorized access, destruction, use, modification, and disclosure. Further, organizations should take reasonable security measures appropriate to the level of risk associated with the improper loss of, or improper access to, the collected personal data; they should meet or ideally exceed current consensus best practices, where available. Organizations should secure personal data at all stages, including collection, computation, storage, and transfer of raw and processed data.
5. **Access and Correction:** Users should have qualified access to personal data that they have provided, and to rectify, complete, amend, or delete this data. This access and ability to correct should be reasonable, given the context of the data flow, appropriate to the risk of privacy harm, and should not interfere with an organization's legal obligations, or the ability of consumers and third parties to exercise other rights provided by the Constitution, and U.S. law, and regulation.
6. **Risk Management:** Users should expect organizations to take steps to manage and/or mitigate the risk of harmful uses or exposure of personal data. Risk management is the core of this Administration's approach, as it provides the flexibility to encourage innovation in business models and privacy tools, while focusing on potential consumer harm and maximizing privacy outcomes.

[4] Source: https://www.ntia.doc.gov/files/ntia/publications/fr-rfc-consumer-privacy-09262018.pdf. Introduction is our own commentary; principle headings and descriptions are directly quoted from NTIA source document.

7. **Accountability:** Organizations should be accountable externally and within their own processes for the use of personal information collected, maintained, and used in their systems. As described in the High-Level Goals for Federal Action section, external accountability should be structured to incentivize risk and outcome-based approaches within organizations that enable flexibility, encourage privacy-by-design, and focus on privacy outcomes. Organizations that control personal data should also take steps to ensure that their third-party vendors and servicers are accountable for their use, storage, processing, and sharing of that data.

WEF (World Economic Forum) Customer Data Governance Principles, 2018[5]

The WEF developed a set of data principles based on extensive discussions with representatives from around the globe from the public sector and multiple parts of the private sector. The intent was to create principles that could achieve global agreement and be used to help assure that national and regional laws and regulations will be shaped under assumptions that are as similar as possible while also reflecting differences of views and situations across the different jurisdictions. The high level principles shown below are supplemented with further detail in the full report. Oliver Wyman provided analytical, writing, and process support to the WEF.

- **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."
- **Security:** "Companies should be held responsible and accountable for data security."
- **Personalization:** "Companies should be able to create individual customer-level profiles that allow them to provide differentiated customer services."
- **Advanced Analytics:** "Companies should be able to comprehensively test, validate, and explain their use of data analytics and models to customers."
- **Portability:** "Companies should, where appropriate, allow customers to access, download, transfer and/or permit third parties to manage data about them."

HOW SHOULD FINANCIAL DATA RIGHTS BE REGULATED?

Designing the best achievable system for governing financial data rights requires making a series of decisions. The "right" answers depend on the legal system and culture of a jurisdiction, existing regulatory structures, and choices about prioritization. Some of the key considerations are:

Roles of general data regulators versus financial regulators. If there are one or more general data regulators in a jurisdiction, then there will need to be a formal division of responsibility for financial data regulation with existing financial regulators. This could involve a carve-out for financial data, a delegation of some aspects to financial regulators, some form of dual coverage, or clear subordination of the financial regulators to the general data regulators on this topic.

Proper balance of law, regulation, supervision, and self-regulation. Data governance can be prescribed by laws, delegated to regulatory bodies to create specific regulation, left to the discretion of supervisors who apply law and regulation, or placed in the hands of self-regulatory

[5] Source: http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf. Introduction is our own commentary; principle headings and descriptions are directly quoted from WEF source document.

bodies in the industry. In this respect it is no different than other types of financial law and regulation, such as capital requirements or risk management.

Regulation of processes versus outcomes. In common with other types of regulation, there is the question of how much to focus on ensuring the right processes are followed by firms, as opposed to focusing on outcomes, such as the presence or absence of data breaches.

Acquisition of the appropriate expertise. Whichever regulators and supervisors are responsible for financial data, they will need to have access to the right level of expertise on data and on finance. This can be drawn from employees with the right knowledge and experience, external providers, associations of public or private sector entities, etc.

WHAT HAVE COUNTRIES AND REGIONS DONE TO DATE?

There is wide diversity in existing laws and regulations on data rights around the world. Some of the most significant laws and regulations are summarized below.

European Union (EU): GDPR (General Data Protection Regulation), 2016[6]

GDPR is a comprehensive and "consumer-centric" model that focuses on protecting consumer data sovereignty as a human right. Our own brief summary is below.

- **Scope:** broad scope covering any business that processes the data of an EU resident; includes controllers and processors. The regulation applies fully to both government and private-sector entities.
- **Consumer rights:** extensive bundle of rights granted to consumers, including the right to have data erased and the right to not be subject to decisions based solely on automated processes.
- **Lawful basis:** data must be collected for specified, explicit and legitimate purposes, which must be communicated to the consumer; strong conditions for consent, including clear and accessible forms and ease of withdrawing consent.
- **Data sharing:** grants consumers the right to transfer data to other controllers, so long as the controller meets certain security standards; controllers can still transfer certain data without a consumer's explicit consent; transfer to other jurisdiction is enabled, provided those jurisdictions meet certain prerequisites.
- **Security:** data processing should be adequate, relevant, and limited to what is necessary; privacy by design/default required; requires the appointment of data protection officers.
- **Enforcement regime:** very strict enforcement regime, including revenue-based fines, broad supervisory powers granted to regulators, and greater risk of private claims; process-oriented regulation, requiring ongoing demonstration of compliance; mandatory notification of data breaches by responsible data controller.

[6] Sources: http://www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf; https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-13.pdf..

China: Cyber Security Law, 2017 (Rule making/implementation ongoing)[7]

China's Cyber Security Law is much more focused on national security than others and imposes stringent consent requirements on data collectors. Our own brief summary is below.

- **Scope:** applies to "network operators" (any companies that maintain computer networks to operate businesses or provide services in China) and "operators of critical information infrastructure" (generally companies that provide communications and information services, energy, finance, or transportation), with a very broad definition of "sensitive personal information" that brings with it heightened requirements.
- **Lawful basis:** businesses must give clear and specific notice and obtain opt-in consent before collecting any personal information (more stringent requirements for "sensitive personal information"); purpose limitations are required (data limitation).
- **Data sharing:** permits some international data sharing, however certain sensitive data must be stored domestically.
- **Security:** includes specific and rigorous requirements related to security testing and procedures for entities that process personal information, reflective of a broader commitment to data privacy as a matter of national security in the policy; specific appointed data privacy officials are required.
- **Enforcement regime:** many different categories and levels of penalties exist, the most severe being the revocation of licenses and fines of around $155,000.

California: CCPA (California Consumer Privacy Act), 2018[8]

The CCPA is mostly focused on providing consumers with additional rights, rather than creating a comprehensive regime of data protection and security. Our own brief summary is below.

- **Scope:** The CCPA applies to companies that do business with California residents; some exemptions for data already affected by federal regulation, such as Gramm-Leach-Bliley for banks. The regulation does not apply to government entities (though some are calling for an expansion of the regulation to cover such entities).
- **Consumer rights:** The primary impact of the CCPA is to provide new rights to California residents, including the right to:
  - Know what specific information is being collected about them;
  - Know whether their personal information is sold or disclosed and to whom;
  - Say no to the sale of personal information (opt-out);
  - Obtain a copy of personal information that has been collected on them;
  - Receive equal service and price, even if they exercise their privacy rights.
- **Enforcement regime:** imposes new penalties for data breaches and enables individuals to take legal action.

[7] Sources: https://www.csis.org/analysis/new-china-data-privacy-standard-looks-more-far-reaching-gdpr; https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr; http://www.mondaq.com/china/x/714616/Data+Protection+Privacy/An+Overview+of+Chinas+New+Cybersecurity+Law.

[8] Sources: Internal OW documents; https://www.irmi.com/articles/expert-commentary/a-summary-of-ccpa-of-2018.

Australia: Open Banking Initiative, 2018[9]

Australia finalized its plan to bring open banking to the country in 2018, with implementation beginning in mid-2019. Our own brief summary is below.

- **Scope:** Initially will apply to the "Big 4" Australian banks. These banks will begin by sharing all credit/debit card and deposit/transaction account data (July 2019), then mortgage data (Feb 2020), then essentially all consumer financial data (July 2020) with authorized third parties when requested by the consumer. Smaller banks must meet these requirements on a 1-year delay.
- **Consumer rights/data sharing:** Consumers will only have the right to request that banks share their data with other authorized third parties (open data), not initiate payments (open process), or transfer accounts (open products). In turn, authorized third parties will have to share any "equivalent" data they possess about the consumer with the bank. There will be no right to deletion.
- **Lawful basis:** informed and explicit consent will be required for all information sharing.
- **Security:** a graduated, risk-based accreditation standard will be used to assess whether third parties meet requirements to receive data, though a minimum set of security standards must be met.
- **Enforcement:** enforcement will be regulated by a government entity, the Australian Competition and Consumer Commission.

[9] Sources: https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf; https://www2.deloitte.com/au/en/pages/financial-services/articles/open-banking.html..

CONCLUSIONS

The financial sector is being transformed by changes fueled by a huge growth in the volume of data and the sophistication of analytical techniques applied to that data. In parallel, the public and their political representatives and associated regulatory authorities, have begun to realize that the public policy infrastructure of laws, regulations, and oversight approaches has not kept pace with this transformation. We collectively need to rethink public policy in regard to data rights and obligations. This primer has hopefully helped lay out the questions. We are committed at Oliver Wyman to help the public and private sectors find appropriate answers.

We further believe that a true global conversation that involves both the public and private sectors is an important part of this process of finding good answers, which is why we have been working with the World Economic Forum and other groups to further that conversation.

ABOUT OLIVER WYMAN

Oliver Wyman is a global leader in management consulting. With offices in 50+ cities across nearly 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 5,000 professionals around the world who help clients optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities. Oliver Wyman is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC].

For more information, visit www.oliverwyman.com. Follow Oliver Wyman on Twitter @OliverWyman

www.oliverwyman.com