DIGITAL ECONOMY

ENABLING ENVIRONMENT GUIDE

KEY AREAS OF DIALOGUE FOR BUSINESS AND POLICYMAKERS

This publication was funded in part by the National Endowment for Democracy

The **Center for International Private Enterprise (CIPE)** strengthens democracy around the globe through private enterprise and market-oriented reform in order to expand access to opportunity for all citizens and create democracy that delivers. By improving the business climate for entrepreneurs and tearing down legal and regulatory barriers through policy advocacy, including the use of technology, CIPE has supported the private sector to be driving forces for reform. By working with private sector organizations globally, CIPE is helping businesses find their voice in policymaking on a range of digital economy issues, including open internet. **www.cipe.org**

The New Markets Lab (NML) is a non-profit center for law, development, and entrepreneurship that houses comparative expertise and an international team of lawyers focused on socially accountable economic legal and regulatory reform. NML sees law as a driving force that can generate entrepreneurship and economic development. Economic laws and regulations need to be clear and accessible, particularly if small businesses, women, and the poor are to benefit from economic growth. Without rules that are better designed and applied and trained lawyers who can solve problems in a new way, most markets tend to be open only to those with the resources to impact decision-making. The organization has developed a unique approach and set of legal tools that give the economically disadvantaged a more direct role in shaping regulatory systems and provide hands-on training for young lawyers from developing and developed countries alike. **www.newmarketslab.org**

Disclaimer: This publication by the Center for International Private Enterprise (CIPE) and the New Markets Lab (NML) provides general information related to the current policy and regulatory environments on the digital economy based on research. The publication is meant for informational purposes only. This publication does not provide legal advice of any kind and should not be used as a substitute for obtaining legal advice. Although CIPE and NML have gone to great lengths to make sure the information in this guide is accurate, neither organization can guarantee that the information is complete or up-to-date. CIPE and NML strongly recommend that readers consult a licensed attorney if they require legal advice.

Acknowledgements

Editor

LOUISA TOMAR, Program Officer of Global Programs, CIPE

Lead Authors

KATRIN KULHMANN, President & Founder, New Markets Lab

MEGAN GLAUB, Senior Legal Fellow, New Markets Lab

MENGYI WANG, International Legal Specialist, New Markets Lab

Contributors

KIM ERIC BETTCHER, Ph.D., Director of Knowledge Management, CIPE

ANNA KOMPANEK, Director of Global Programs, CIPE

LOUISA TOMAR, Program Officer of Global Programs, CIPE

MORGAN FROST, Assistant Program Officer of Global Programs, CIPE

ANA MARÍA GARCÉS ESCOBAR, Legal Fellow, New Markets Lab

ADITI RAO, Legal Fellow, New Markets Lab

LANXIN CHEN, Legal Intern, New Markets Lab

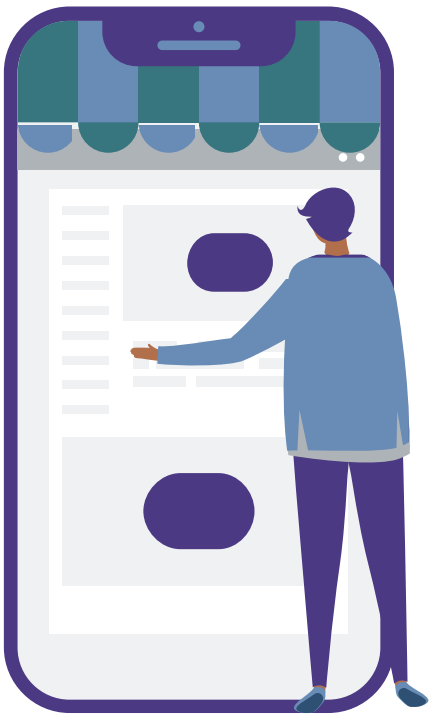
A special thank you to
Brian Bieron, Executive Director, eBay Inc. Public Policy Lab
and a Board Member of the Center for International Private Enterprise.

Table of Contents

Part I – Digital Economy Summary Guide

Introduction

The expanding digital economy, which includes cross-border services and electronic commerce (e-commerce), can be an important driver of democratic and economic development by opening up new market channels for local business, promoting inclusive trade, and boosting tax revenue for governments to increase access to essential services. As digital innovation spreads around the globe, local business communities, particularly in the Global South, continue to face barriers to overcoming technological and digital divides. National policies, laws, and regulations governing this new space heavily influence development outcomes. Local businesses and organizations that represent them must be equipped to advocate an enabling environment that promotes inclusive growth in a digital future.



To that end, the Center for International Private Enterprise (CIPE) and New Markets Lab (NML) joined forces to create this Guide meant to support policy dialogues on topics crucial for strengthening inclusive digital business environments around the world.

Presently, there is no consensus on a set of harmonized global norms and standards to guide and align regulatory change for the digital economy. Therefore, it is imperative that local business communities and like-minded reformers understand and address the complex digital systems evolving at the international, regional, national, and sometimes sub-national levels. The global economy continues to shift into the digital sphere, while the rules and regulations that enable the digital economy are still in nascent stages in many countries, often hindering both local growth and access to world markets. At the same time, technological innovation and cyber risks are outpacing the development of national strategies and increasingly require novel approaches and greater international cooperation.

As economic activity increasingly takes place online, local business communities must have a say in how the rules and regulations for e-commerce and digital trade are designed and implemented to ensure their participation and sustainability on- and offline. All too often the frameworks governing the digital economy are driven by governments, with minimal input from stakeholders like small and mid-sized firms, whose voices are essential to inclusive economic development.

At the same time, many governments are seeking to achieve the United Nations Sustainable Development Goals (SDGs) through technology-focused initiatives and partnerships such as the 2030 Vision,[1] a platform established by the United Nations Global Compact, the British Council, and others for dialogue and collaboration to understand the potential for digital to deliver the SDGs and to explore the role the technology sector can play supporting other industries' efforts. There has never been a better moment for local business communities to join this democratic dialogue to ensure that their needs and concerns are considered.

This Guide aims to explain the complex legal and regulatory aspects of the digital economy for all stakeholders, regardless of their technical knowledge or policy experience. It is divided into two parts:

- **Part One: Digital Economy Summary Guide** starts with a definition of the digital economy and identifies the Guide's many audiences, including local business communities, regulators, and civil society. It offers insights on leveraging the Guide and avenues for advocacy and dialogue. The four priority topics covered – **Consumer Protection, Data Protection, Cybersecurity, and Electronic Transactions (e-payments and e-signatures)** – were selected through an assessment and ongoing discussions with CIPE partners in emerging and frontier markets. The four topics are defined and discussed in the context of business advocacy and each section contains a checklist for assessing existing national legal and regulatory frameworks. The Summary Guide concludes with information on the methodology developed by NML and a call to action for democratic dialogue.

- **Part Two: Legal Deep Dives**, include more detailed information on **International and Regional Frameworks** applicable to each of the four digital economy topics; examples of different **Regulatory Approaches** used around the world; considerations for **Implementation and Enforcement** of laws and regulations; and the **Institutional Frameworks** that exist for each.

1. *2030 Vision – Technology Partnerships for the Global Goals, https://www.2030vision.com/get-involved/2030vision-uniting-to-deliver-technology-for-the-global-goals2. International Monetary Fund, Measuring the Digital Economy. p. 6. Web. April 5, 2018.*

The Digital Economy

What exactly does "digital economy" mean? This Guide adopts a broad definition: the digitalization of the economic activity that incorporates data and the internet "into production processes and products, new forms of household and government consumption, fixed-capital formation, cross-border flows, and finance."[2]

The digital economy has become a ubiquitous element of daily life in most countries. The rapid diffusion of the internet has altered how businesses operate and transact with consumers, how citizens obtain public services, and how regulators work at the domestic and international levels. Digitization is giving rise to new business models, new cross-border supply chains – and new risks. Goods and services marketed online, digital content, and data analytics are fast becoming globally traded commodities.

Like the internet itself, the digital economy is truly global; it has no borders, and those who are able to connect can immediately access markets across the world. The nature of this economy gives rise to unique questions regarding how to regulate it. Traditional approaches to protect consumers, honor contracts, and store information need to be reassessed for the digital realm. Moreover, laws, regulations, and policies governing the digital economy must work in concert with efforts to boost the operational environment, including IT infrastructure, services, platforms, ecosystems, and devices. For instance, reliable electricity, telecommunications networks, and optical fiber are all critical infrastructure to be addressed alongside legal and regulatory issues.

Although many factors affect the digital economy, this Guide focuses on four priority areas: (1) **consumer protection**, (2) **data protection**, (3) **cybersecurity**, and (4) **electronic transactions, specifically electronic payments (e-payments)** and **electronic signatures (e-signatures)**. Together, these topics constitute much of the enabling environment for the digital economy and affect nearly every aspect of conducting business online in a responsible and secure manner. Individually and collectively, these issues can act as force multipliers for broader reform and are central to both business opportunity and government concern.

2. *International Monetary Fund, Measuring the Digital Economy. p. 6. Web. April 5, 2018.*

Is this Guide for Me?

The Guide focuses on the four priority areas listed above from the perspective of **local business communities**, including **entrepreneurs** and **small and medium-sized enterprises** (SMEs). It aims to provide the most fundamental information needed to understand the current policy landscape, enhance compliance with rules, and spot issues for ongoing dialogue and reform. While not prescriptive, it discusses how to identify opportunities for advocacy and dialogue with policymakers to develop an inclusive digital economy.

This Guide is also designed to provide the local business community, including **business associations**, **chambers of commerce**, and **economic think tanks** (especially in emerging and frontier markets) with a framework for understanding the major concepts that make up the legal and regulatory environment surrounding the digital economy.

In addition, this resource seeks to supplement the knowledge needed by **policymakers** and **regulators** to develop and implement effective policies and regulations. The Legal Deep Dives cover each of the four focus topics by going in-depth into regulatory considerations and existing international frameworks.

All stakeholders, including **international** and **civil society organizations**,[3] can use this tool to help identify key intervention points and opportunities for engaging local business and government in dialogue. The Guide addresses the existing rules surrounding the digital economy, provides a foundation for policy advocacy based on best practice, and supplies a shared language for much-needed multi-stakeholder dialogue.

3. *It is helpful here to briefly note the difference between laws, regulations, and policy. Laws (or acts), which often must go through a parliamentary process, create a framework for governing the market and often relate to a particular sector or activity. Laws tend to be more general and create legally enforceable obligations. Regulations are created, often through administration action, to implement laws and tend to be both more detailed and also easier to change. Policies, which are the broadest category of measures, provide guidance to stakeholders and government officials on what objectives laws and regulations should seek to achieve but do not tend to be legally binding instruments on their own.*

Leveraging the Guide

Technology changes so rapidly that without a proper mechanism, public-private engagement on digital economy issues will never keep pace. Depending on the local circumstances, public policy priorities may be new laws and regulations, or better implementation of existing rules. In all cases, democratic dialogue requires stakeholders bringing well-prepared messages to policy discussions.

Preparation involves understanding and prioritizing the high-level themes that this Guide outlines, weighing the positions that business can take, mapping like-minded stakeholders, and clarifying desired outcomes. By articulating priority issues and concrete outcomes, local business communities can move beyond a list of broad questions to focus on interventions that could influence how the digital economy is shaped domestically and globally. Developing knowledge on the key themes can also provide a foundation for a wide range of stakeholders to share thoughts on policy objectives and priorities, highlighting that inclusive dialogue does not just satisfy particular interests but supports broader economic and social development objectives.

Policy Advocacy and Dialogue

What is Advocacy?

The digital economy is a priority area for local business to engage with business organizations such as chambers of commerce, business associations, and economic think tanks that can be valuable conduits for policy advocacy. Advocacy is an effort to influence and engage in public policy in an open, transparent manner. As a tool of civil society, it addresses issues of broad concern to the community and makes the case for change by presenting evidence and support from civic constituencies. Advocacy supports decision-making while informing and empowering the public. Through advocacy, the private sector shares essential practitioner information and perspectives with government on markets and the business operating environment. Government benefits from this grassroots-level input on the economy in order to understand the effects of its policy choices.

What is Public-Private Dialogue?

Public-private dialogue (PPD) is a structured, participatory, and inclusive approach to policymaking. Dialogue improves the flow of information relating to economic policy, in this case the digital economy, and builds legitimacy into the policy process. It also seeks to overcome impediments to transparency and accommodate greater inclusion of stakeholders in decision-making.

While the technical and regulatory characteristics of the digital economy explored throughout this Guide may be new to many policymakers and business advocacy groups, the Center for International Private Enterprise (CIPE) has decades of experience supporting local reformers and private sector participation in democratic dialogue and public policy reform efforts.

Advocacy Questions to Guide Strategy

- **What needs to be changed?**
- **Who can make the changes?**
- **How much change should be made?**
- **When should the changes be made?**
- **How can the case for change be made?**
- **How will the changes be implemented?**

Source: CIPE, How to Advocate Effectively: A Guidebook for Business Associations

Over the past 35 years, CIPE has supported more than 1,000 local initiatives in more than 100 developing countries, and created numerous publicly available resources including the National Business Agenda (NBA)[4] and a PPD toolkit to assist with participatory policymaking efforts around the globe. This Guide serves as both a tool for approaching the advocacy process and as a regulatory and legal resource for private and public sector counterparts to develop a shared language for the initial stages of dialogue.

The key to initiating productive dialogue is to find a wedge issue – an issue of wide current interest that prompts action and opens the door for addressing related areas of strategic importance.[5] An example of a wedge issue in the digital economy could be anything from concerns over a problematic new data localization requirement to the need for more widespread implementation of an e-signature law recently passed in parliament. Preparation for serious dialogue takes months, during which the business community must assess policy challenges and options, mobilize stakeholders, and formulate positions.

Chambers of commerce and business associations require methods to collect and process input from the business community on its needs and objectives. These may differ substantially depending on whether a business provides goods or services online or neither. Input can be gathered in multiple ways, including surveys, focus groups, and outreach to association and coalition members. It is necessary to collect information on the many challenges facing local business – not just multinationals or technology companies – and identify possible solutions. Forming consensus on policy positions can be challenging because businesspeople may have diverse interests in the digital economy. The key is to balance competing demands and prioritize shared objectives.

4. *CIPE. National Business Agenda Guidebook. Web. 2006.*
5. *Bettcher, Kim E. (CIPE) Making the Most of Public-Private Dialogue: An Advocacy Approach. Web. 2011.*

Business organizations embarking on advocacy efforts should also engage the broader business community and civil society to acquire mutual understanding and allies. Coalitions, founded on a common interest – for example, expanding e-commerce access for local SMEs – may incorporate different sets of supporters depending on the issue. Whether coalitions are temporary or permanent, all members must present a common message to credibly influence public policy. When forming coalitions to create a more inclusive digital economy, it is important to consider allies such as start-ups, civil society organizations, open internet advocates, technology companies, and multilateral organizations such as the United Nations Commission on Trade and Development (UNCTAD).

Dialogue is always followed by implementation steps and policy monitoring. This includes pressure for follow-through from the private sector and other supporters. It is also important that the business community consider the pace of technological change when assessing desired policy outcomes – the speed of innovation necessitates a continuous analysis of the effectiveness of current laws and regulations.

In order to keep a broad coalition of reformers engaged, there must be a means of reporting to constituencies on the outcomes of dialogue and educate the community about new policies and rules. Reform requires an ongoing effort that builds on earlier achievements. After each phase of dialogue, it is important to assess the lessons and opportunities that emerged, refine advocacy strategies, and prepare for the next phase. Over time, these efforts can foster a more inclusive democracy and digital economy.

3 Keys to Successful Advocacy:

1. **CONSTITUENT INTEREST – consult with and listen to association and coalition members before establishing the target advocacy issue(s).**
2. **WIDEST BENEFIT – avoid issues that concern narrow interests and give priority to issues that affect multiple sectors of the economy.**
3. **FEASIBILITY – concentrate advocacy efforts in policy areas where there is a good chance of achieving positive results or at least mitigating negative impact.**

Checklist for Stakeholder Representation in the Policy Advocacy Process[6]

- [ ] Survey membership or coalition about the most important or pressing digital economy issues
- [ ] Determine and analyze the current laws and regulations that apply to the priority issues
- [ ] Define the official position of the membership and/or coalition based on evidence and analysis
- [ ] Identify the key decision-makers and influencers (industry sector, government ministry/regulatory body, etc.)
- [ ] Determine best method of communication to reach decision-makers and influencers
- [ ] Prepare communication materials and messages (radio, social media, etc.) supported by research and facts
- [ ] Implement the advocacy campaign and track progress and achievements
- [ ] Evaluate the effectiveness of the campaign and assess implementation of policy or regulatory change

6. *For additional guidance on advocacy see: https://www.cipe.org/vba/business-associations-guidebook/*

   https://www.cipe.org/legacy/publication-docs/advocacyguidebook_english.pdf

Understand the Issue – Consumer Protection

Consumer protection is an important area of law that protects individuals and enterprises who purchase goods and services through electronic and non-electronic means. Consumer protection laws seek to shield consumers from "improperly described, damaged, faulty, and dangerous goods and services as well as from unfair trade and credit practices."[7]

Consumer protection in e-commerce is essential to fostering a trustworthy environment online. Having a strong consumer protection regime in place would also benefit the local business community – for example, across business-to-business (B2B) transactions – by enhancing trust in e-commerce, simplifying digital transactions, and expanding the consumer base. Creating a baseline understanding of the rights and obligations for protecting consumers online will help local businesses and advocacy groups engage in an ongoing policy dialogue in this emerging area.

At present, conventional consumer protection regimes are often not designed to address new practices, such as advertising on social media. As a result, many governments do not have the right protections in place. Regulation of consumer protection in e-commerce focuses on key questions: (1) **how to balance rights and obligations among stakeholders** (governments, industry, and consumers), and (2) **how to integrate e-commerce-specific considerations into conventional consumer protection regimes**. Regulations tend to correspond to the three main stages of consumer transactions: the pre-purchase phase (duties to disclose and advertising), payment phase (terms and conditions of transactions, transparent/secure payment, and data protection), and delivery/after-sale phase (dispute resolution and redress and the right to withdraw/cancel or cooling-off period). (See **Diagram 1**).

Diagram 1. Regulatory Elements of Consumer Protection

Source: New Markets Lab (2018)

7. *Your Dictionary, Consumer Protection Law – Legal Definition. Web.*

One particularly important part of consumer protection is dispute resolution. Dispute resolution is crucial for enterprises and consumers alike, given that merchant-customer disputes frequently arise in electronic transactions at the post-sale phase. SMEs in developing markets often cite compliance with consumer protection laws and relevant dispute resolution measures as a challenge for growing their digital presence.[8] A major stumbling block is enforcement of laws and regulations that might already exist. This was the case in Peru (see case study below). To streamline enforcement, governments and businesses alike are increasingly turning to alternative means of dispute resolution, especially online dispute resolution (ODR). For example, both Mexico and Brazil have rolled out government-backed ODR mechanisms. In the private sector, enterprises such as eBay, Alibaba, and PayPal all have versions of ODR.

Despite the importance of clear consumer protection regimes for both businesses and consumers, consumer protection is often one of the last areas that developing economies focus on regulating as they create frameworks around e-commerce. Internationally, consumer protection has also not received the focus it deserves, and there is little consensus on standards. Clear and adequately enforced laws and regulations are important for companies to build trust with consumers – especially in predominantly cash-based economies where trust is typically built face-to-face. Given the global nature of the digital economy, comparability across domestic legal and regulatory frameworks would greatly ease the burden on businesses and regulators alike. Global harmonization around the elements of consumer protection would help create standard expectations among consumers and common rules for merchants, creating increased legal certainty and trust overall.

8. *International Trade Centre, New Pathways to E-Commerce; a Global MSME Competitiveness Survey. Web. September 25, 2017.*

Case Study:
Online Dispute Resolution in Peru

Although a jurisdiction may have a strong and comprehensive set of laws related to consumer protection and contract enforcement, without equally strong legal institutions, neither consumers nor the business community will have confidence to transact. Such was the case in Peru, where an inefficient court system made enforcing consumer protection regulations difficult, with negative impact on trade and investment overall. A partnership between the state-owned development bank Corporación Financiera de Desarrollo (COFIDE) and the non-profit Innovations for Poverty Action (IPA) helped improve the situation.

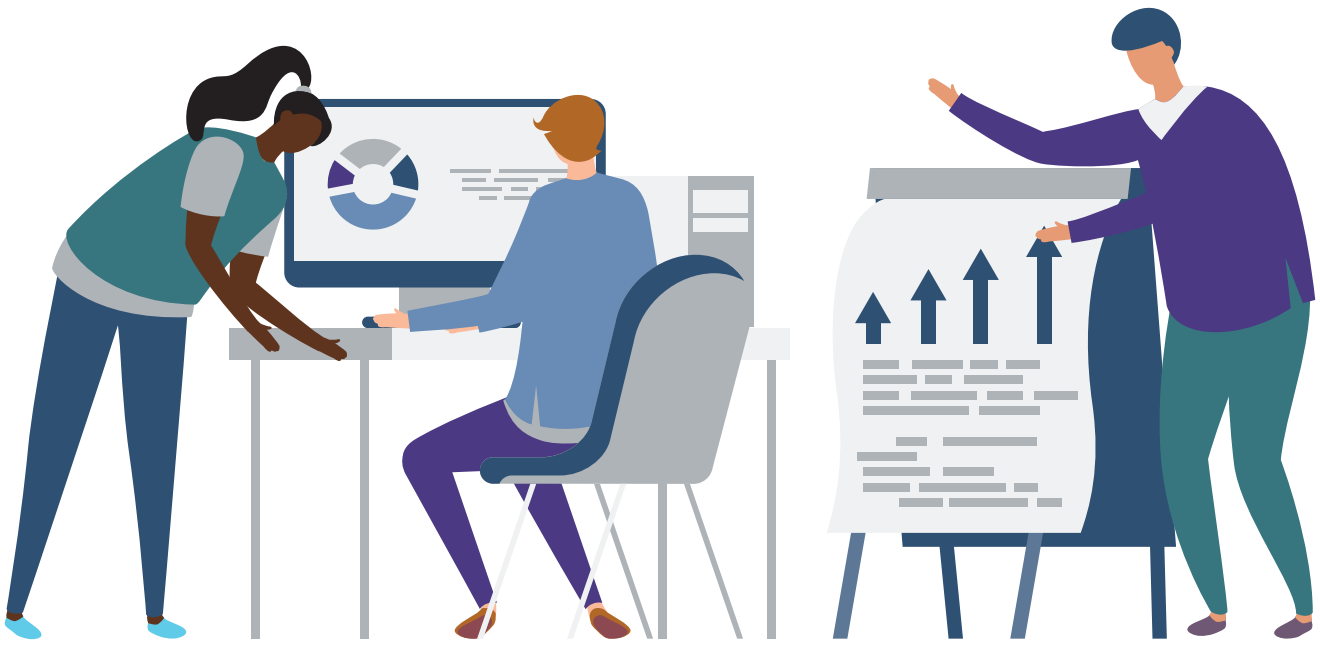
COFIDE and IPA collaborated to create a pilot online dispute resolution platform that incorporates user-driven inputs like a penalty mechanism, evaluations, and ratings to enhance contract enforcement in Lima's Gamarra district, home to Latin America's largest garment cluster. The ODR system has been especially helpful given Peru's economy, which – although one of the fastest growing in Latin America – is still small and largely informal. Business communities facing similar problems could emulate this approach by partnering with the public sector and civil society organizations with goals of strengthening consumer confidence and trust in the judiciary incrementally while providing a model for more institutionalized rule of law reform.

Source: FHI360, The Atlas of innovation for Economic Stability, Web, May 2018.

Guidance for Business and Recommendations

To better understand their legal obligations, local businesses should first understand where the responsibilities lie for consumer protection. Responsibility tends to be allocated across industry (particularly e-commerce platforms and online vendors), regulators, and consumers. Each stage of a transaction – pre-purchase, payment, and after sale/delivery – has different regulatory considerations with different responsibilities. Understanding the rules at each stage of the transaction and engaging in self-regulation could add to brand quality and further increase the likelihood of consumer engagement, while minimizing risk and reputational fallout in the case of a dispute. The business community should also examine whether there are e-commerce-specific business activities that are not covered by an existing regulatory regime (for example, advertising on social media) and consider whether these activities should be included in an advocacy approach.

Initiatives to address consumer protection in a global marketplace exist, but they tend to be general in nature and do not provide sufficient guidance to enterprises, governments, or consumers. Business advocacy groups looking to engage in this area could work with policymakers and other advocates to create specific initiatives, provisions, and measures that suit the needs of consumers (e.g., protection from counterfeit or fraudulent goods) and businesses (e.g., protection from intellectual property or trademark infringement).



As the local business community navigates the legal and regulatory landscape for consumer protection, four priority regulatory considerations could help structure business models and inform advocacy efforts.

These are 1) **degree of business liability for e-commerce platforms**, 2) **dispute resolution,** 3) **an established right to withdraw/cooling off period**, and 4) **institutional structures for regulating consumer protection in e-commerce.**

- **Degree of Business Liability:** E-commerce platforms face different obligations from their brick and mortar counterparts, such as information verification and supervision, which can present a heightened degree of liability. Depending upon specific market conditions and the local business climate, different approaches may suit business, consumer, and government needs. In mature markets with a high concentration of businesses, more stringent obligations may be appropriate and well understood. However, similar obligations in smaller, more fragmented markets, could delay or disadvantage new entrants to e-commerce ready platforms, as has been the case for economies in the Association of Southeast Asian Nations (ASEAN).

- **Dispute Resolution:** Dispute resolution mechanisms are particularly important, since merchant-customer disputes and B2B disputes routinely arise in digital transactions. While litigation (including through small claims courts) is one possibility, it may not be the best option in all jurisdictions. ODR provided by public or private actors, as well as mediation and arbitration, could be more effective approaches for resolving disputes efficiently.

- **Right to Withdraw/Cooling-Off Period:** Another priority area for enterprises and consumers is the right to withdraw/cancel (cooling-off period), which allows consumers to cancel online orders within a certain period of time. The exact length of the period varies across jurisdictions, and the business community should become familiar with the exceptions to the right to withdraw. Advocacy can be tailored to the needs of specific sectors.

- **Institutional Structures for Regulating Consumer Protection in E-Commerce:** In many countries, a specific regulatory body for consumer protection in e-commerce has yet to be established. Having a dedicated regulator can help ensure that regulations will reflect local market needs and can provide businesses with a focal point for advocacy efforts. One approach is the creation of special consumer protection units within an existing regulatory institution (consumer protection agency) tasked with meeting challenges online.

Checklist for Analyzing Existing Consumer Protection Laws and Regulations

Who regulates online consumer protection in your jurisdiction (ministry, regulatory body, etc.)? Is there a dedicated regulatory body or unit for online consumer protection?

Has online consumer protection been incorporated into existing consumer protection laws, or does a law specific to online consumer protection exist?

If not, are there new draft laws, regulations, or policies that address online consumer protection issues?

Who is responsible for enforcement of consumer protection laws and regulations within your jurisdiction?

When disputes arise, is the enforcement mechanism in your jurisdiction able to resolve these issues in a fair and timely way?

Has your country adopted or encouraged an online dispute resolution (ODR) framework? Are ODR mechanisms commonly used within the local business community?

Do businesses self-regulate to ensure consumer protection?

Are there existing avenues for public-private dialogue on online consumer protection? Are there currently opportunities for the private sector to work alongside regulators and policymakers to create and uphold consumer protection laws?

Are businesses notified when a draft law is being developed, and is there an established process for providing comments?

Have you engaged with frameworks regulating consumer protection at the regional or international level?

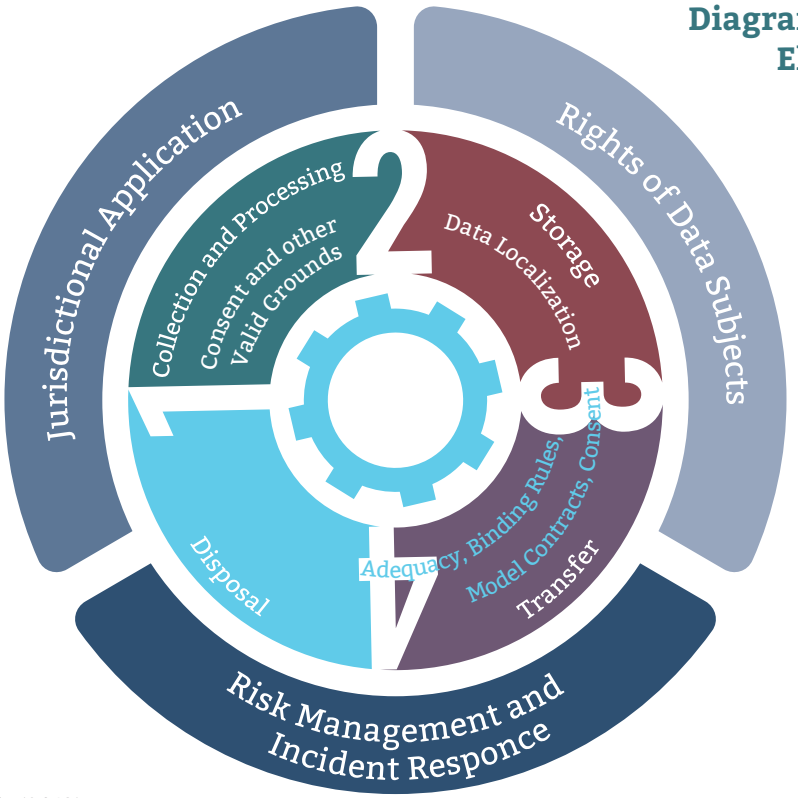
Understand the Issue – Data Protection

The digital economy has helped drive the creation and international circulation of an unprecedented amount of data. Data protection regulations relate to both individuals who purchase goods and services electronically and companies that buy, sell, or provide services online by protecting the data that is submitted through these transactions. Data protection serves multiple purposes such as privacy and security and has traditionally been a focus of national regulations, due in part to the strong national security concerns of governments.

Characterized as the oil of the digital economy, data have become a key global commodity and are increasingly harnessed, processed, exchanged, and analyzed in massive quantities to power digitalized content, goods, and services. Data protection has thus become a focal point for the business community, regulators, and consumers alike. All data follow a lifecycle – data collection and processing, storage, transfer, and disposal – which underpins most regulatory approaches around the globe (see **Diagram 2**). Regulation tends to follow the steps in the data lifecycle, and enterprises may have different obligations depending upon their specific business model. Regulations also often include cross-cutting obligations, such as responses to a data breach.

Countries around the world are increasingly recognizing the crucial importance of data and are enacting data protection laws in response. For governments, regulating data requires a delicate balance among several factors: national security, surveillance,

Diagram 2. Regulatory Elements of Data Protection Regimes



Source: New Markets Lab (2018)

competition policy, innovation, the integrity of electoral process, and consumer protection. Individuals are also worried about how their personal data will be collected and used, particularly in sensitive areas such as biometric data. For example, some individuals may be concerned with advertisements for commercial or political purposes that target them based on personal data. Many are also concerned about government surveillance.

As of July 2018, 107 countries had enacted data protection laws. Other countries with large and growing markets for digital goods and services (such as Kenya, Brazil, Nigeria, and Egypt) are currently drafting bills to protect data. Participation and comment throughout the drafting process is an important way for the business community to make its voice heard (see case study on page 23). Like with consumer protection, there is no internationally recognized standard to guide the development of national regulations on data protection. Not only does this affect the business community, which must sometimes design separate data protection procedures to comply with regulations in different jurisdictions, but it also has a meaningful impact on a regulator's ability to enforce data protection laws. The lack of harmonization presents a timely opportunity and common wedge issue for public-private engagement. In order to most effectively engage in this dialogue, the private sector could become familiar with other countries' legal regimes that may serve as models for domestic legislation or encourage policymakers and business associations to focus on international policy initiatives.

For businesses, the specific requirements for protecting data will be fundamental. For example, regulations on registration and fees should not be overly burdensome, and requirements to provide internal controls like a data protection officers may disproportionately impact smaller businesses. In addition, the issue of data localization (requirements that companies build local data centers to store data or in some instances store a copy of data locally) has been met with criticism from the private sector.

Companies of all sizes want to leverage the massive quantity of available data to provide innovative goods and services and, as highlighted in a recent CIPE publication, can use robust data protection systems to boost brand reputation and build trust with consumers and users.[9] Globally, common ground is emerging for how to safeguard the interests of smaller enterprises and consumers while promoting innovation and growth. Advocacy groups that work with both SMEs and larger enterprises can use these approaches to build a diverse agenda.

Differences in the degree to which countries regulate data protection also impacts cross-border data flows, which tend to reflect one of two main approaches, each with different implications for the private sector: 1) **an approach focused on the adequacy of regulations in the country exporting the data**, which emphasizes the soundness of a country's legal regime and places the burden on the public sector, or 2) **a binding corporate rules approach**, which assesses the degree to which a company has in place an effective independent review mechanism to protect data and places the burden on the private sector. Although the later may seem less appealing, it is not necessarily a bad option.

9. *CIPE, Why Companies in Emerging Markets Should Prioritize Data Privacy. Web. April 6, 2018. 017.*

Case Study:
Commenting on Data Protection Acts in Panama

Business associations can actively participate in the legislative process for data protection laws. Even though the process itself varies considerably across jurisdictions, administrative processes sometimes allow for engagement and comments from civil society and private actors. One example is the development of data protection legislation in Panama.

In mid-2016, the Panamanian Congress presented a bill regulating data protection in the country. It held a three-month-long public hearing to receive comments from civil society actors, private citizens, and businesses. The public hearing was conducted by the Innovation National Authority (Autoridad Nacional para la Innovación Guvernamental in Spanish) and the Transparency Agency (Autoridad Nacional de Transparencia y Acceso a la Información in Spanish) and had the special participation of the Organization of the American States and the Interamerican Court of Human Rights, meaning that regional and international frameworks were considered. Participants provided comments, which were included in the final bill presented to Panama's Congress in February 2017. To promote public discussion on the matter, different organizations held conferences with a large private sector representative (like Google) and the Panamanian Chamber of Commerce.

As of 2018, the bill has not yet been adopted into law due to budgetary constraints. Nevertheless, the rulemaking process in Panama highlights a good practice whereby interested business associations were welcomed to actively participate in the rulemaking process and voiced their concerns, and regional and international institutions and companies were involved to contribute additional insights and support dialogue. Similarly, in India and Kenya, Data Protection Bills are currently open for public comment.

Sources: IPANDETEC, Cronología de un Proyecto de Ley de Protección de Datos en Panamá, Jan. 29, 2018. Web; AIG, Consulta pública sobre Proyecto de Ley de Protección de Datos de Carácter Personal" refuerza el marco legal para la Economía y el Gobierno Digital, July 11, 2016, Web. Violeta Villar, Panamá necesita aprobar Ley de Protección de Datos, El Capital, Feb. 14, 2018. Web; Gobierno de Panamá, Avalan proyecto que establece la protección de datos de carácter personal, Consejo de Gabinete, Jan. 18, 2017, Web.

Guidance for Business and Recommendations

As a first step, local business communities should understand the range of laws, regulations, and other measures that are applicable to them with respect to data protection; this will depend upon both where the data subjects involved reside and the relevant stages in the data lifecycle (collection, processing, storage, or transfer). Due to the lack of international harmonization, local businesses can be subject to laws and regulations in multiple jurisdictions. Companies may need to design separate data protection systems, such as terms of service, to accommodate different national regulatory requirements. While this might not be an issue for larger enterprises, it places a heavy burden on SMEs. Working together through business associations or chambers of commerce can be an effective way for SMEs to ensure that their particular needs are considered.

Advocates for the business community should also rally behind a common approach to cross-border data transfer. There are several notable considerations, with implications for those in the business community seeking to expand into foreign markets. First is whether data protection laws only apply domestically or also reach overseas enterprises when they collect or process data of domestic residents (Japan's system is one example of the latter). A second consideration is the degree to which the local business community or national policymakers are engaged in broader discussions at the international level. Advocates could press for greater international harmonization and/or a sustained focus on making international frameworks and institutions better incorporate the needs of SMEs, for example. With respect to regulatory harmonization, there are some good models that exist – for instance, efforts to streamline certifications between the European Union (EU) and APEC – but these are not yet widespread.

As the local business community navigates the legal and regulatory landscape of data protection, six priority regulatory considerations could help structure business models and inform advocacy efforts. These are 1) **the scope of the regulatory regime**, 2) **the degree to which data protection laws are focused on the consumer**, 3) **levels of data protection that vary based on company size**, 4) **institutional structures for regulating data protection**, 5) **approaches to cross-border data transfers**, and 6) **exceptions to data protection regimes.**

- **Scope of Regulatory Regime:** Regulatory regimes for data protection vary and can be tailored to the nature of the local market. For example, while some countries have adopted more comprehensive overarching regulations on data protection (such as the EU, Japan, and Ghana), others regulate based on the data protection needs of different sectors or functions. South Korea is an example of the latter, with different laws applying to information technology (IT), financial transactions, and the disclosure of personal credit information.[10] While Brazil currently takes a similar approach, there are two draft laws under consideration that would move the country toward a general data protection framework.[11] As more jurisdictions begin to change or update their legal frameworks, the private sector's participation in the rulemaking process will become increasingly important.

- **Consumer Focus:** Some influential legal frameworks, like the EU's General Data Protection Regulation (GDPR),[12] take a consumer-centric approach to data protection that requires enterprises to provide more control and a range of rights to consumers. For example, in the EU and Russia, more stringent requirements apply to sensitive data. Certain categories of consumers, such as children, may also be afforded higher levels of protection (for example, the Child Rights Act No. 26 of 2003 in Nigeria protects the privacy of children under 18). The business community can learn from these examples and incorporate key takeaways as appropriate within their jurisdiction.

- **Levels of Compliance that Differ Based on Company Size:** The capacity and data impact of the business community is also a common consideration; some jurisdictions have created laws and regulations with differing levels of compliance to accommodate the capacity of different sized business. For example, in Australia, businesses with an annual turnover of AU$3 million or less (with certain exceptions) are not subject to the Privacy Act. This is an especially relevant consideration for SMEs and startups.

10. *DLA Piper, Data Protection Laws of the World: South Korea. Web. January 16, 2017.*
11. *Bruno Bioni and Renator Leite Monteiro. Brazilian General Bill on the Protection of Personal Data. IAPP. Web. January 31, 2018; Bill 5276/2016 Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Web.*
12. *Regulation (EU) 2016/679 of The European Parliament and Of The Council Of 27 April 2016 on The Protection of Natural Persons with Regard to The Processing Of Personal Data And on The Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).*

- **Institutional Structures for Regulating Data Protection:** Establishment of a clear regulatory institution responsible for data protection could provide a point of contact for the business community and the public, streamline rules, and avoid challenges and costs due to overlapping regulations. In some jurisdictions, new regulatory entities or special units within existing regulatory institutions have been founded to address specific challenges related to data protection. These units could be limited in duration and scope, and support efforts to move towards a more general system of regulating data protection.

- **Approaches to Cross-Border Data Transfers:** The best approach to cross-border data transfers may ultimately depend upon the strength of national data protection laws. In jurisdictions with weak data protection laws, the local business community may actually prefer the binding corporate rules approach, which relies upon companies to put in place internal mechanisms and can result in stronger enforcement.[13] On the other hand, if an enterprise is located in a jurisdiction with strong data protection rules, it could request that its government seek 'adequacy status' from another jurisdiction, which would streamline data transfer overall.

- **Exceptions to Data Protection Regimes:** In jurisdictions where data protection requirements may place a high compliance burden on enterprises, particularly SMEs, the business community could advocate exemptions from certain rules and work with governments to modify these requirements. Further exceptions to consider include, appointment of an internal data protection officer (based on company size), reduction of excessive registration fees, or elimination of data localization requirements.

13. *The model contracts approach, which looks at the wording within specific contracts and determines whether it sufficiently protects the data transfer, would also be an option, but it is used less frequently (to date, it is used only in the EU and depends upon full implementation of model contracts). See United Nations Conference on Trade and Development, Data Protection Regulations and International Data Flows: Implications for Trade and Development. 13. Web. 2016.*

Checklist for Analyzing Existing Data Protection Laws and Regulations

Who regulates data protection in your jurisdiction (ministry, regulatory body, etc.)?

Does your country or territory have data protection laws or regulations? Draft laws or regulations?

If your jurisdiction has a data protection law or laws, do the ministry/regulatory bodies take a more general approach to data protection, or are different sectors regulated differently?

Who is responsible for enforcement of data protection laws and regulations within your jurisdiction?

Is your sector or industry most concerned with a particular aspect of the data protection lifecycle?

Is your sector or industry concerned with a particular user demographic?

Do businesses self-regulate to ensure data protection? Is there a mechanism to rectify data breaches publicly?

Are there existing avenues for public-private dialogue on data protection? Are there currently opportunities for the private sector to work alongside regulators and policymakers to create and uphold data protection laws?

Have you engaged with frameworks regulating data protection at the regional or international level?

Have you experienced issues with respect to cross-border data protection? If so, do you know how they have been approached?

Understand the Issue – Cybersecurity

Cybersecurity regulation, which protects information technology and computer systems from attack, is a global concern that is relevant to all members of the business community and everyone engaged in online activity. In recent years, attacks on computers and information networks, both public and private, have grown in scale and severity, harming governments, industry, and consumers. Cybersecurity includes the assets of both public and private actors and covers "connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information."[14] While the digital economy and e-commerce in particular have been able to deliver inclusive growth, constantly evolving technologies can lead to vulnerabilities on the internet that require robust and resilient cybersecurity systems.

The regulatory framework for cybersecurity has evolved in three stages: (1) **cybercrime legislation at the national level**, (2) **standards and guidelines initiated by the private sector**, and (3) **the recent shift towards broader legislation that comprehensively regulates cybersecurity** (See Diagram 3 below). The business community should be aware of the cybersecurity framework within its home jurisdiction and determine where gaps may exist. Public and private actors should work in concert to determine appropriate regulatory approaches and sequencing of reforms, taking into consideration both the compliance burden placed on enterprises (particularly SMEs and startups) and the needs of consumers.

Diagram 3. Evolution of Cybersecurity Regulations

Cybercrime Legislation

First type of cybersecurity regulation adopted in most through a top-down approach. Most common cybercrimes include:

- E-Mail Spoofing
- Phishing
- Spamming
- Cyber-Defamation
- Cyber Stalking
- Identity Theft
- Software Piracy
- Unauthorized Access
- Denial of Service
- Web Defacing
- Ransomware
- Salami Attack
- Logic Bomb
- Data Diddling

Private Sector Led Multi-Stakeholder Enforcement

Private development of cybersecurity program, procedures, and standards is institutionalized through a multi-stakeholder framework

Comprehensive Cybersecurity Regulation

Recently enacted overarching regulations address:

- Coverage (general or sector specific)
- The preventive aspect (strategic, organizational, and monitoring mechanisms), and
- The reactive aspect (definition of cyber incident or cyberattack and legal obligations triggered by cyber incident or cyberattack)

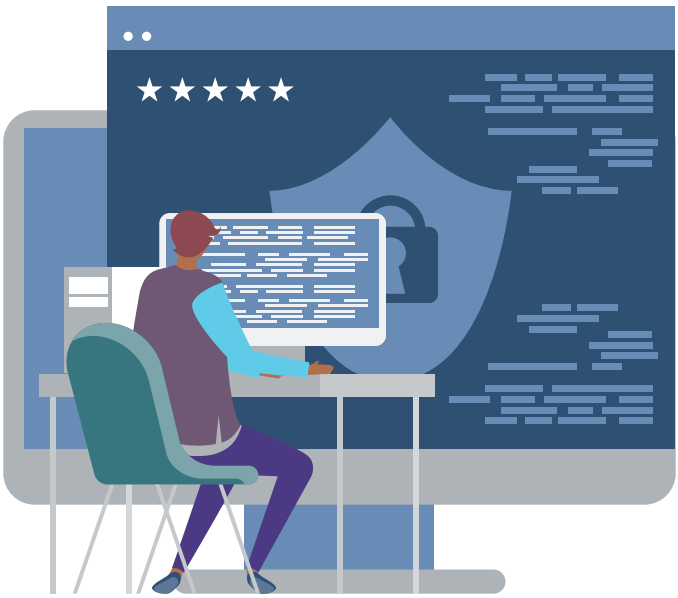
Source: New Markets Lab (2018)

14. *International Telecommunications Union, Definition of Cybersecurity. Web.*

Cybercrime legislation, which criminalizes a range of digital crimes like hacking and identity theft, is the most common approach and can be effective when accompanied by appropriate sanctions and strong enforcement. The local business community could help focus and prioritize interventions by aligning industry best practices with the legal regime as well as through public-private initiatives. The business community should consider the policy purpose behind the recent movement toward enactment of comprehensive cybersecurity regulations as well as potential burdens. Regulators will likely continue to roll out more stringent and detailed rules and standards, which will strengthen cybersecurity but also create additional compliance obligations. It will be important for the local business community to press regulators to find the correct balance.

Cybersecurity legislation that is comprehensive but not over-reaching could include the following components: designation of entities that are critical to national security with balanced requirements placed on those entities and their information systems; risk management-based approaches for companies in line with global best practices that take business structure and assets into account; and measures to reduce the frequency and magnitude of cyberattacks on systems that are key to economic growth. Extraneous provisions to watch out for in cybersecurity legislation include an obligation to monitor online expression, pre-launch audits of hardware and/or software, long criminal sentences for breaches, and data localization requirements. In addition, establishing a Computer Emergency Response Teams (CERT) – common throughout the Americas, can facilitate quick incident reporting and recovery efforts for the business community as well as for critical infrastructure and government agencies.[15]

Overly prescriptive approaches may present challenges for the business community, which would be best served by a system that allows for flexibility in adopting relevant standards. Both the business community and regulators could benefit from the creation of incentives for enterprises to adopt best practices. Such a bottom-up approach would place less of an enforcement burden on regulators, while allowing SMEs to build capacity to enhance consumer confidence. Recognizing the equivalence of comparable existing standards would also ease the regulatory burden on the local business community. Importantly, the business community should participate in the standard-making and harmonization process to ensure that its needs are addressed (see the case study below). The business community might also look to relevant international and regional frameworks to guide application of best practices and help shape their approach to advocacy.



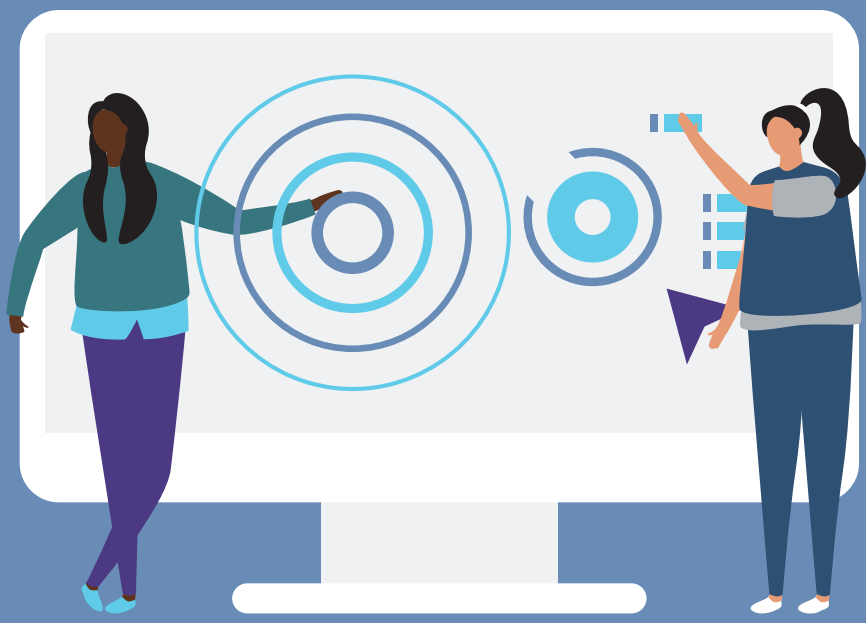
15. *https://www.sites.oas.org/cyber/EN/Pages/Directory/Default.aspx*

Case Study:
Public-Private Coordination on Cybersecurity in Tunisia

In Tunisia, the National Agency for Computer Security (NACS) was created in 2003 under the Ministry of Communication Technologies. The NACS is tasked with executing the national strategy in ICT security, performing periodic risk assessment, and setting up the Cert-Tunisian Coordination Center (Cert-TCC) that provides assistance with information security. Cert-TCC has multiple missions, including informing the public of cyber incidents and threats, promoting capacity building, and aiding the national, regional, and international communities with identifying vulnerabilities of products and systems.

Most promising for the business community, the Cert-TCC is also tasked with facilitating communication between public and private sector actors, in particular experts and professionals in the technology field and business associations focused on cybersecurity. Cert-TCC has helped establish discussion forums and capacity building programs to connect these different stakeholders. The Cert-TCC also promoted public-private cooperation through the Saher-HoneyNet, an initiative that uses a preventative approach to mitigate cyber threats and also promotes inter-agency enforcement.

Nonetheless, more remains to be done to align Tunisia's approach with international cybersecurity standards. The business community within Tunisia might encourage further capacity building efforts by its government focused on strengthening compliance with international standards.



Sources: Tunisian National Agency for Computer Security. History of The Creation of The Agency Web; Jidaw, Tunisia Information Security strategy – National Agency for Computer Security. Web.

Guidance for Business and Recommendations

A robust and resilient cybersecurity system is crucial to addressing vulnerabilities on the internet. Regulations in this field have evolved through three stages, as discussed above, and public and private actors should work in concert to determine, adopt, and implement the appropriate balance of regulations and flexibility. This process should take into consideration the compliance burden for the local business community (particularly SMEs and startups), policy objectives, and the needs of consumers and citizens.

As the local business community navigates the legal and regulatory landscape for cybersecurity, five priority regulatory considerations could help structure business models and inform advocacy efforts. These are 1) **the scope of the cybersecurity regulatory regime**; 2) **incentives for adopting industry best practices**; 3) **institutional structures for regulating cybersecurity**; 4) **enhanced enforcement of cybersecurity frameworks**; and 5) participation in international and regional frameworks.

- **Scope of Cybersecurity Regulatory Regime:** Regulatory regimes for cybersecurity vary across the three main phases discussed above (cybercrime law, private sector-led multi-stakeholder enforcement, and comprehensive cybersecurity laws). For example, many countries have laws on cybercrime but are still developing more overarching cybersecurity laws. As more jurisdictions begin to change or update their legal frameworks for cybersecurity, the private sector's participation in the rulemaking process will become increasingly important. Public-private dialogues could benefit a broader range of stakeholders including open internet advocates and financial institutions, and the local business community should determine whether appropriate channels for these dialogues exist at the national level.

- **Incentives for Adopting Industry Best Practices:** As formal legal systems shift to more comprehensive focus on cybersecurity, industry-led efforts based on best practices can be an important way to address cybersecurity concerns and boost consumer confidence. Best practices can be shared through approaches like multi-stakeholder initiatives, clear implementation guidelines, and tailored adoption of model laws and regulations. These initiatives could help enterprises gain more information on standards and prioritize steps for adopting best practices, both of which would be particularly helpful for SMEs with limited capacity and underinvestment in cybersecurity. Regulators could also create incentives for enterprises to adopt best practices (for example, voluntary guidelines and certification programs).

- **Institutional Structures for Regulating Cybersecurity:** Establishment of a single regulator to manage all institutional functions related to cybersecurity could facilitate compliance, streamline regulation, build capacity (in both the public and private sectors), and avoid challenges and costs due to overlapping regulations. Examples from some jurisdictions, such as Tunisia, which has created a central regulator, and Sri Lanka, where sector specific units have been founded to meet specific challenges, could provide useful discussion points for public-private engagement.

- **Enhanced Enforcement of Cybersecurity Frameworks:** Proper enforcement of existing frameworks for cybersecurity at all levels (domestic, regional, and international) is also a key point. This should include advocacy for collaboration and harmonization across the different enforcement agencies responsible for different aspects of cybersecurity and enhanced international cooperation.

- **Enhanced International and Regional Frameworks:** The business community could advocate to strengthen international and regional frameworks, which tend to be general and center around capacity building and information sharing. While important, these are only first steps and not enough to effectively deal with global cybersecurity concerns. Increased international focus could also facilitate domestic rulemaking and could be pegged to the three stages of cybersecurity regulation (cybercrime laws, private sector-led initiatives, and comprehensive cybersecurity legislation) to guide countries that are at different stages of development.

Checklist for Analyzing Existing Cybersecurity Laws and Regulations

Who regulates cybersecurity in your jurisdiction (ministry, regulatory body, etc.)? Is there a single regulatory body that manages all issues related to cybersecurity or are functions split across institutions?

Does your jurisdiction have laws on (1) cybercrime and/or (2) cybersecurity more generally? Is there a national security law that address aspects of cybersecurity?

If not, are there draft laws under consideration to address aspects of cybersecurity?

Who is responsible for enforcement of laws and regulations related to cybersecurity in your jurisdiction? Are penalties appropriate to deter infringement but not too excessive that it deters reporting?

Are there voluntary guidelines and certification programs that guide industry self-regulation?

What hardware, software, and organizational requirements for addressing cybersecurity apply to the local business community?

Are there existing avenues for public-private dialogues on cost effective approaches to cybersecurity? Are there currently opportunities for the private sector to work alongside regulators and policymakers to create and uphold cybersecurity laws?

Are businesses notified when a draft law is being developed, and is there an established process for providing comments?

Have you engaged with frameworks regulating cybersecurity at the regional or international level?

Understand the Issue – Electronic Transactions (E-Payments and E-Signatures)

E-commerce underpins much of the digital economy. E-commerce is similar to the traditional exchange of goods and services and includes digital transactions and agreements between actors along the supply chain. Within electronic transactions, different issues arise, such as how to enter into a fair contract or receive payment without face-to-face interaction or how to resolve disputes between parties. This section of the Guide covers two areas of particular importance to electronic transactions: electronic payments (e-payments) and electronic signatures (e-signatures).

E-payments are an essential part of doing business for every company and consumer engaged in online transactions, and e-signatures are the fundamental element of electronic contracting, which is now emerging as a substitute for handwritten contracts. Both e-payments and e-signatures come with different challenges and hurdles, and the business community should remain engaged in the rulemaking process and openly communicate with government to ensure that their needs are met.

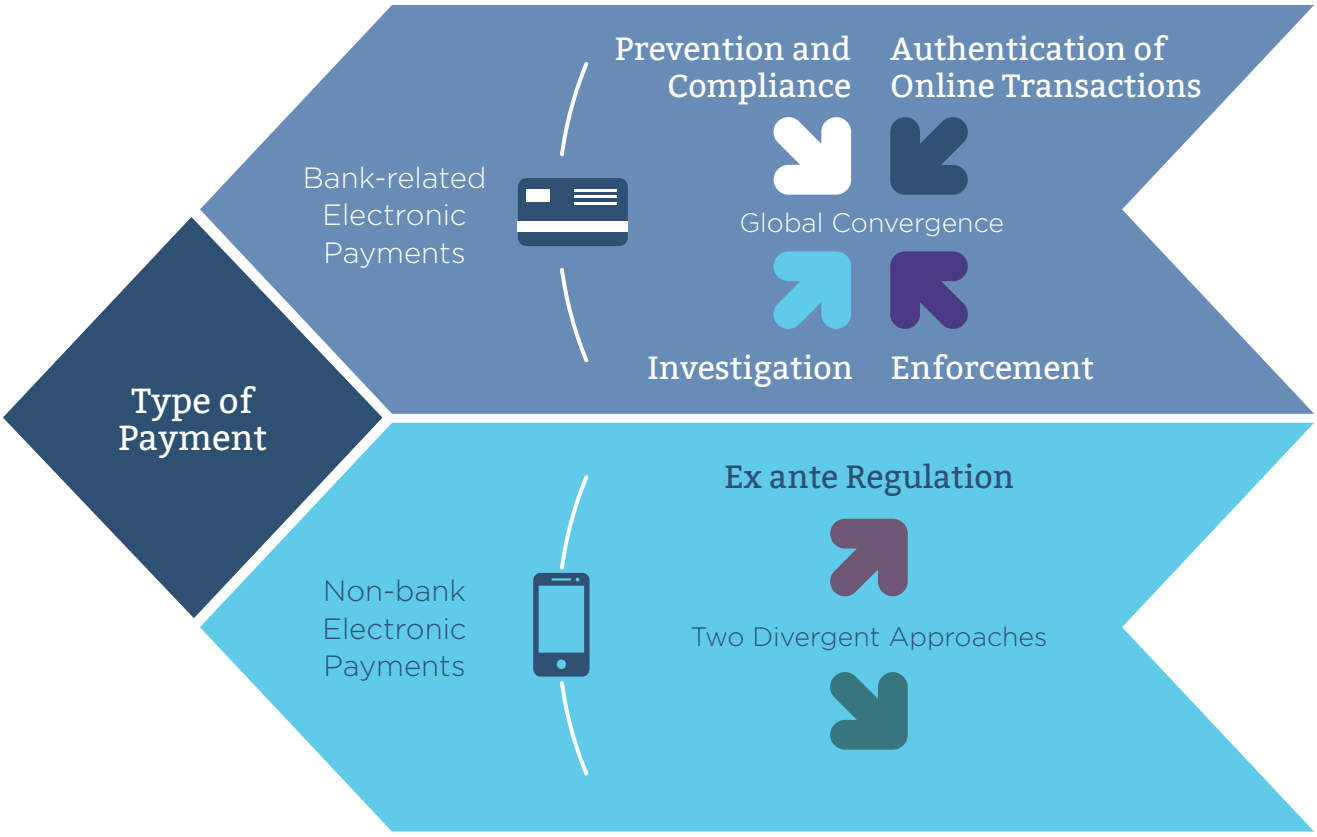
E-Payments

E-payments are an integral part of the digital economy and have become widely adopted in recent years thanks to technological innovation and the massive penetration of mobile phones and smartphones throughout the world. There are many types of e-payment systems, but they can broadly be categorized under one of two groups: bank-related e-payments and non-bank e-payments. Bank-related e-payments include the more traditional e-payments like Automated Clearing House (ACH) payments and credit and debit cards and are connected to banking systems through various types of bank accounts. Non-bank e-payments are provided by non-bank intermediaries include newer, more innovative methods such as PayPal, Alipay, and Google Wallet.

E-payments are not without challenges, especially when operating across borders and financial systems. Both parties to a transaction want assurance that payments will come through without delay, and governments must make sure that transactions protect those with less market power. Common priorities for both the public and private sectors include prevention of fraud, as well as security issues at the transactional level. As a result of the different stakeholders and considerations involved, regulators tend to focus on regulations for e-payments. Prioritizing the development of institutional infrastructure that can investigate problems as they arise and enforce rules in the case of a violation is also a key consideration for governments.

Depending upon the type of e-payment system used, there are several approaches to regulations (See **Diagram 4** below). Overall, bank-related e-payments are heavily regulated across the globe, and policymakers tend to use similar elements (prevention and compliance, authentication of transactions, investigation, and enforcement). In contrast, regulatory systems for non-bank e-payments often follow one of two approaches: 1) an **ex ante approach,** which contains requirements for entering and operating in the market through either case-by-case regulatory approval or broader measures, and 2) an **ex post approach** which uses less restrictive conditions for market entry, and is more focused on enforcement once enterprises are operating in the market.

Diagram 4. E-payment Regulatory Approaches



Source: New Markets Lab (2018)

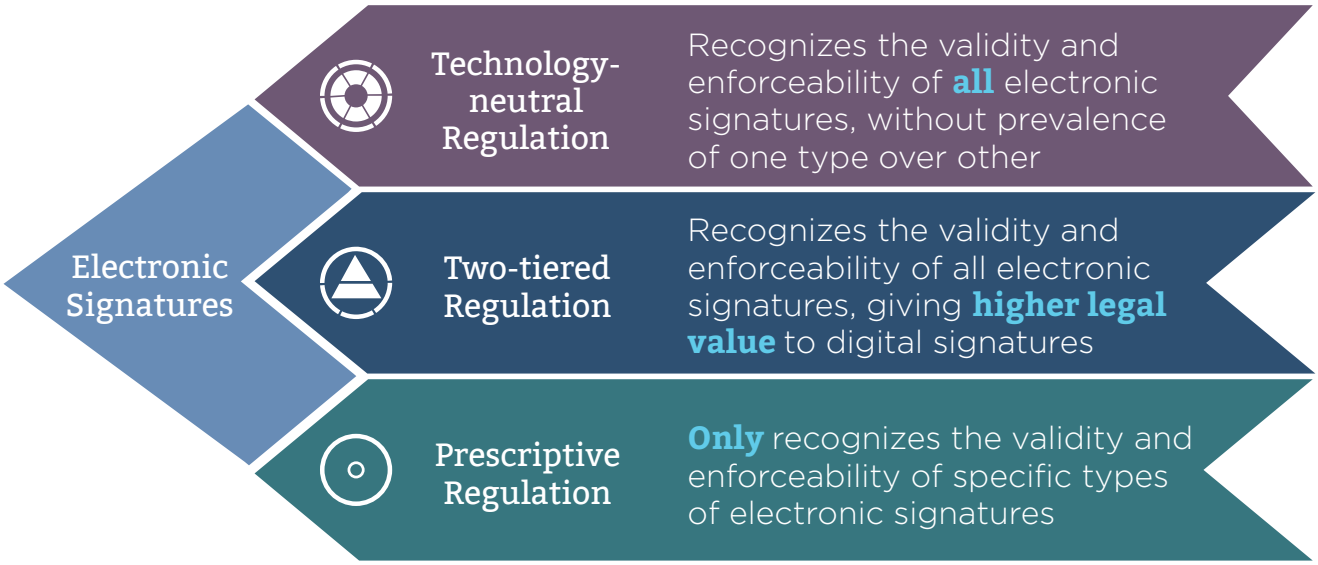
E-Signatures

Clear rules around e-signatures – which, like handwritten signatures, signal that the parties have agreed to an enforceable contract – are becoming increasingly important in the digital economy. E-signature regulatory systems provide assurance that both the buyer's and seller's obligations are valid, legal, and enforceable. However, the local business community should not only consider the legal framework itself but also focus on its implementation, as e-signatures sometimes continue to be treated differently despite legal frameworks that recognize them.

E-signatures are typically regulated in three different ways: 1) **technology-neutral regulations** view all types of e-signatures and handwritten signatures as equal; 2) **two-tiered regulations** recognize the legality and validity of multiple types of electronic signatures but consider digital signatures authenticated by certain technologies more legally significant; and 3) **technology-specific regulations** recognize only limited types of e-signatures (these are prescriptive regulations). The institutional framework to enforce electronic signatures varies depending upon which regulatory approach the jurisdiction follows and could include third-party certification bodies.

Although e-signatures are becoming more widely recognized, some regulatory bodies (for example, Sri Lanka) and courts in various jurisdictions (for example, Ghana) have shown resistance when it comes to accepting e-signatures, highlighting the need for further multi-stakeholder engagement (see case study on page 37). Internationally, most instruments that regulate electronic contracts and electronic signatures recognize the functional equivalence between handwritten and e-signatures and aim to harmonize national laws. The United Nations Commission on International Trade Law (UNCITRAL) has developed a model law that provides guidance on harmonizing rules under a technology-neutral approach, which would facilitate digital trade and better address the needs of the business community in emerging and frontier markets.

Diagram 5. E-Signature Regulatory Approaches



Source: New Markets Lab (2018)

Case Study:
Electronic Signatures in Sri Lanka

In 2006, Sri Lanka passed the Electronic Transactions Act. No. 19 (ETA), which recognized the legality and validity of e-signatures; however, "bureaucratic resistance to change and administrative lethargy" impeded the implementation of the Act for over 10 years. This is a prime example of a key issue in legal reform: the difference between enacting a law and its implementation.

Verité Research, an interdisciplinary think tank and partner of CIPE, worked with the Import Section of the Ceylon Chamber of Commerce (CCC) to advocate implementation of Sri Lanka's ETA, which authorizes the use of digital signatures and digital documents in export-import processes. In consultation with CCC's members, Verité discovered that Sri Lankan exporters continued to face onerous requirements to submit hard copies of trade paperwork, and few business leaders were aware of the ETA's provisions. Following rounds of meetings with stakeholders in business, the legislature, and the civil service, Verité and CCC produced and distributed a policy report. The report and related discussions raised awareness among exporters and government officials that provisions authorizing e-documents and e-signatures within the ETA outweighed other legislation requiring hand-written signatures for authentication.

Verité and CCC met with government officials including the National Trade Facilitation Committee to discuss the report's findings and key recommendations. As a result, the 2017 and 2018 federal budgets included proposals to digitize government systems and the government reformed a 148-year-old customs ordinance paving the way for electronic document (e-document) processing platforms and shorter customs procedures. These improvements could ultimately lead to an increase in Sri Lanka's general trade competitiveness.

Source: Financial Times, Accepting E-Documents with E-Signatures: A Small Step for the Govt, A Giant Leap for The Country. Web. 2017; Lanka Business Online, Verité Wants Govt to Issue Guidelines on E-Signature. Web. 2017.

Guidance for Business and Recommendations

E-payments

Existing regulatory approaches to e-payments must balance different policy and stakeholder considerations. E-payment options can involve high compliance costs with negative implications for business viability, particularly when smaller firms rely on third-party services. While some aspects of e-payment regulation acutely impact enterprises that provide e-payment services, the information included in this Guide applies to the business community as a whole. Rules related to the types of e-payment services available in the market and the degree to which they suit business needs, will directly impact all enterprises engaged in e-commerce. Likewise, relevant regulations applicable to banking institutions, which tend to be heavily regulated across the globe, will affect the availability of bank-related payment solutions.

In some jurisdictions market entry is heavily regulated (ex ante regulation), while in others businesses are expected to self-regulate, with the public sector heavily focused on enforcement. Even in jurisdictions that follow an ex ante approach, the local business community could work with regulators to establish "Regulatory Sandboxes" to test out their products without legal uncertainty. Regulatory Sandboxes provide safe spaces for the business community to experiment with more innovate business structures and products. They also promote lower cost innovative services and help producers reach the market faster. Several jurisdictions use this model already, and it could be adapted to new markets as well.

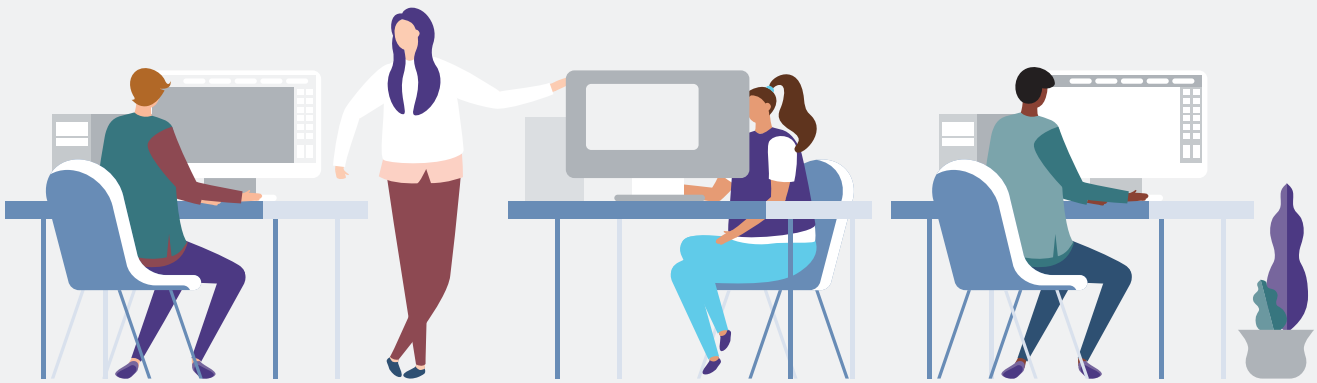
As the local business community navigates the legal and regulatory landscape for e-payments, four priority regulatory considerations could help structure business models and inform advocacy efforts. These are 1) **the range of applicable regulations**; 2) **institutional structures for regulating e-payments**, 3) **regulatory experimentation** (and "Regulatory Sandboxes"); and 4) **enhanced engagement in international and regional frameworks**.

- **Institutional Structures for Regulating E-Payments:** While e-payments tend to be covered under existing regulatory institutions, greater focus on the particular challenges that arise in an e-payment context would be beneficial. Some jurisdictions have created new regulatory entities or special units within existing institutions to focus specifically on e-payments, and these institutional approaches could provide useful discussion points for public-private dialogue.

- **Range of Applicable Regulations:** E-payments tend to be covered under several regulatory schemes, spanning both bank-related payments (which link to a complex web of financial regulations) and non-bank-related payments. The local business community using (or providing) bank-related payment solutions needs to be aware of the range of applicable regulations and the associated compliance requirements. Although non-bank financing options tend to be less heavily regulated, the line between bank-related and non-bank-related finance is not always clear. The business community should work with regulators to better understand this divide and, where relevant, move regulators away from burdensome frameworks, taking cues from more flexible jurisdictions.

- **Regulatory Experimentation (and "Regulatory Sandboxes"):** E-payments continue to evolve, and the high degree of innovation in financial technology or 'FinTech' calls for greater collaboration across the public and private sectors. There remains a need to bring more low-cost options to market that promote financial inclusion. This can benefit SMEs which rely on third-party e-payment solutions. One innovation, though unusual, has been to establish "Regulatory Sandboxes" to allow enterprises to engage with regulators around new products and services within a safe space free of legal liability. Whether in the context of a regulatory sandbox or not, the private sector could encourage the adoption of less market restrictive, ex post regulation whenever feasible.

- **Enhanced Engagement in International Frameworks:** Several international frameworks relate to the regulation of e-payments and may provide guidance as countries develop more detailed regulations. In addition, the ongoing WTO Trade in Services negotiations would further open up the financial services sector and provide local businesses worldwide with more affordable e-payment options. SMEs would likely reap significant benefits even if a small group of WTO members were to commit to further liberalization.



E-Signatures

The local business community should also understand the rules regarding different types of e-signatures in the different markets in which they operate, including any exceptions that might apply. Normally the local business community will find technology-neutral regulations to be the least burdensome, but regulatory approaches should be tailored to a specific jurisdiction.

As the local business community navigates the legal and regulatory landscape for e-signatures, four priority regulatory considerations could help structure business models and inform advocacy efforts. These are 1) **the scope of the regulatory regime**; 2) **institutional structures for regulating e-payments**; 3) **enhanced enforcement of e-payment frameworks**; and 4) **adoption of international and regional frameworks.**

- **Scope of Regulatory Regime:** Regulators typically do not use the same approach for different types of e-signatures, the local business community should familiarize themselves with the specific rules and exceptions within their jurisdiction. SMEs might be best served by technology-neutral laws that are easier to comply with and treat e-signatures and handwritten signatures with equal legal significance. Still, clearer enforcement of laws within jurisdictions, particularly those with more complex regulatory regimes could make a big difference to the ease of online transactions.
- **Institutional Structure for E-Payments:** The creation of a single regulator or enforcement body could help provide a point of contact for the business community and streamline creation and implementation of rules and regulations. Examples from some jurisdictions include the creation of special units within existing institutions or new regulatory bodies or entities (this may include, for example, neutral third-party certification agents for e-signature). The institutional structure for e-payments should also take into consideration international and regional norms to make it easier for enterprises to engage in cross-border agreements.
- **Enhanced Enforcement of E-payment Frameworks:** Proper enforcement of existing frameworks for e-payments at all levels (domestic, regional, and international) is also a key point. As in the case of Sri Lanka, some jurisdictions may already have strong laws and regulations on e-payments but that are not effectively enforced. Advocacy may focus on greater collaboration and harmonization across the different enforcement agencies responsible for e-payments as well as enhanced international cooperation.
- **Adoption of International Frameworks:** Wider adoption and implementation of international frameworks, like the UNCITRAL Model Law on E-Signatures – incorporated in domestic laws across Latin America – could provide valuable regulatory guidance and promote harmonization of a technology-neutral approach that better addresses the needs of the global business community. While model laws are guidelines and not "hard law," they nevertheless serve as spring boards for drafting enforceable domestic laws. Alternatively, the technical elements included in the UNCITRAL Model Law can assist business as they engage regulators.

Checklist for Analyzing Existing E-Signature and E-Payment Laws and Regulations

Who regulates electronic transactions in your jurisdiction (ministry, regulatory body, etc.)? Is there a dedicated regulatory body or unit for electronic transactions? Does the same entity focus on both e-payments and e-signatures?

Are there laws, regulations, and policies that specifically address e-payments and e-signatures, or are they enforced under more general contracting and financial transaction laws?

How flexible is your jurisdiction's regulatory framework when it comes to innovative new e-payments services?

Does your jurisdiction treat bank-related forms of e-payments differently from non-bank-related forms of e-payments?

Has your government tried (or does it seem open to) "Regulatory Sandboxes" that could allow businesses to experiment and grow?

Which approach does your jurisdiction take regarding e-signatures (technology-neutral, two-tiered, or technology-specific)?

Have there been administrative or judicial challenges to e-signatures in your jurisdiction?

Are there existing avenues for public-private dialogue on electronic transactions? Are there currently opportunities for the private sector to work alongside regulators and policymakers to create and uphold laws on electronic transactions?

Are businesses notified when a draft law is being developed, and is there an established process for providing comments?

Have you engaged with frameworks regulating electronic transactions at the regional or international level?

Using the Legal Deep Dives

Part II of this Guide contains Legal Deep Dives, which take a more nuanced and comparative look at different regulatory options and approaches within each of the four core issue areas covered above. The Guide follows a methodology developed by the New Markets Lab (NML) to increase awareness of legal requirements and rights. NML's Legal Tools have been used around the world as a mechanism for bringing enterprises and policymakers together to develop a shared understanding of how regulatory systems can be designed and implemented to generate inclusive economic growth. NML's Legal Guides are based on stakeholder needs and have a particular focus on SMEs and marginalized economic stakeholders. To identify the priority topics in this Guide, CIPE engaged in ongoing outreach and dialogue with its local private sector partners around the globe.

NML's Legal Guides do not present specific legal advice, which should be sought through an attorney licensed to practice in a specific jurisdiction, but they do provide a foundation of knowledge about overarching legal and regulatory issues, common considerations that affect SMEs, and possible approaches to improving regulatory design and implementation. NML has been developing Legal Guides since 2012, and has built up a library of region- and stakeholder-focused resources. In some cases, these guides have been used to provide a framework for local advocacy. At the country level, NML has also used tools like Regulatory Systems Maps to break down complex regulatory processes and guide stakeholders through a strategy for identifying and prioritizing intervention points (similar to wedge issues but specifically related to regulatory processes) that may lead to sustainable reform. All NML's legal tools are designed to make legal systems more transparent, inclusive, and democratic.

The Legal Deep Dives in part II of this Guide are not meant to be prescriptive, but rather they detail the legal and regulatory tradeoffs and business perspectives that must be considered in developing any legal framework. All legal systems are different, and a framework that is well suited to one legal system may not work the same way in another. Still, there are many lessons to be learned for both policymakers and the business community, which the comparative approach of this Guide is meant to highlight.

The Legal Deep Dives also outline some of the sample models and frameworks that exist at the international and regional levels, which serve as useful discussion points for the business community. Often, the regional and bilateral frameworks and initiatives contain more detail than models at the international level and include specific examples of solutions to common regulatory challenges. Regulators should use this Guide to find examples of innovative approaches and emerging best practices. The business community can use the Guide to gain a more comprehensive understanding of the complex legal structures that apply to the digital economy in order to improve regulatory implementation and strengthen an informed advocacy approach.

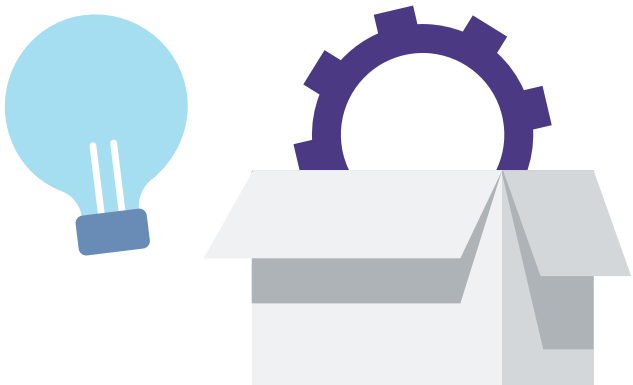
A Call to Action

The interconnected nature of the digital economy means that the interests and risks of businesses, consumers, citizens, and public representatives are deeply intertwined. There are no isolated or domestic digital economies, rather a set of national opportunities and constraints to engage in international digital trade and commerce. For some countries and business communities, consumer protection, data protection, cybersecurity, and electronic transactions may not seem like pressing business or legal considerations. However, inclusive economic growth and development rely on national policies and regulations that facilitate competitiveness in an increasingly digital world. As the scope of digital innovation expands around the globe, local business, especially in the Global South, will face undue barriers to entry and sustainability unless their voices and participation in dialogue and policymaking are heard.

Undoubtedly, the digital economy is challenging to address through policy and regulations because it is highly technical, constantly evolving, and a relatively new area of global commerce. Notwithstanding, democratic policy reform is possible when persuasive, well-reasoned arguments are backed by publicity, grassroots support, and constructive dialogue. Effective advocacy campaigns depend on credibility – establishing a reputation overtime by building bridges across sectors, advocating for the public interest, and engaging in policy reform efforts in a transparent and open manner is crucial. Business advocacy groups may approach digital economy themes by first identifying like-minded stakeholders including startups, universities, and technology-minded civil society organizations or members of government. Broad-based coalitions can secure productive channels of dialogue with the public, the media, and policymakers.

Effective and competitive regulations in the digital age should promote innovation, inclusive economic growth, and increase opportunities for investment and technological collaboration. The benefits of a connected and global marketplace can no longer be limited to a handful of countries and multinational companies. The digital economy may be global but improving the enabling environment for businesses in emerging and frontier markets involves local actors identifying tailored policy recommendations that facilitate their inclusion. By participating in the analysis and formation of the "rules of the game" – the incentives that shape economic behavior and issues affecting long-term development – business can contribute to the design of smart public policy that promotes growth and access to the digital economy.

CIPE and NML hope that businesses and governments alike will heed this call to action to strengthen the enabling environment for a robust and inclusive digital economy.



Additional Resources on Policy Advocacy and Legal Guides

CIPE and NML recommend additional resources listed below to help jumpstart the long and fruitful process of democratic policy reform in the digital age:

- CIPE, How to Advocate Effectively: A Guidebook for Business Associations, 2007, https://www.cipe.org/resources/advocate-effectively-guidebook-business-associations/
- Kim E. Bettcher, Making the Most of Public-Private Dialogue: An Advocacy Approach, 2011, https://www.cipe.org/resources/making-public-private-dialogue-advocacy-approach/
- Kim E. Bettcher, Benjamin Herzberg, Anna Nadgrodkiewicz, Public-Private Dialogue: The Key to Good Governance and Development, 2015, https://www.cipe.org/resources/public-private-dialogue-key-good-governance-development/
- CIPE, Business Associations for the 21st Century http://www.cipe.org/vba/business-associations-guidebook
- CIPE, National Business Agenda Guidebook http://www.cipe.org/publications/detail/national-business-agenda-guidebook-voice-business
- New Markets Lab, East Africa Legal Guide, Aspen Network of Development Entrepreneurs, September 2016, https://docs.wixstatic.com/ugd/095963_54aad2211372409c89cba8790c279912.pdf
- New Markets Lab, Legal Guide for Women Entrepreneurs, Aspen Network of Development Entrepreneurs, update forthcoming August 2018.
- New Markets Lab, Legal Guide to Strengthen Tanzania's Seed and Inputs Markets, with USAID, AGRA, and SAGCOT, 2016, https://docs.wixstatic.com/ugd/095963_3a4f751a4c83488982341082f530aa32.pdf
- New Markets Lab, Working Draft, Transport Services Regulatory Guide, ICTSD, 2016.
- New Markets Lab, Working Draft, Tourism Services Regulatory Guide, ICTSD, 2016.
- New Markets Lab, Working Draft, Information and Communication Technology Services Regulatory Guide, ICTSD, 2016.
- New Markets Lab, Working Draft, Financial Services Regulatory Guide, ICTSD, 2016.

The dialogue process, its lessons and outcomes offer important insights for other reformers in other countries working towards enabling a more inclusive digital economy. CIPE encourages those participating in dialogue and advocacy regarding the digital economy and those using this Guide to share insights and stories with CIPE by tweeting at @CIPEglobal **with the hashtag #DigitalEconomyDialogues.**

Abbreviations and Acronyms

ADR	Alternative Dispute Resolution
AfCFTA	African Continental Free Trade Area
APEC	Asia-Pacific Economic Cooperation
APEC CBPRs	Asia-Pacific Economic Cooperation Cross-Border Privacy Rules
ASAPCP	Strategic Action Plan for Consumer Protection
ASEAN	Association of Southeast Asian Nations
CAUCA	Unified Central American Customs Code
CERT	Computer Emergency Response Team
CIPE	Center for International Private Enterprise
CPTPP	Comprehensive and Progressive Agreement for Trans-Pacific Partnership
CSF	Cybersecurity Framework
ECC-Net	European Consumer Centers Network
ECOWAS	Economic Community of West African States
eLAC2018	Digital Agenda for Latin America and the Caribbean 2018
ENISA	European Union Agency for Network and Information Security
eIDAS	Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market
EU BCRs	European Union Binding Corporate Rules
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
ICPEN	International Consumer Protection and Enforcement Network
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MERCOSUR	Southern Common Market (Mercado Común del Sur)
MPIW	Mobile Payments Industry Workgroup
MSMRs	Micro, Small, or Medium Retailers
NAFTA	North American Free Trade Agreement
NIST	National Institute for Standards and Technology
NML	New Markets Lab
OAS	Organization of American States
ODR	Online Dispute Resolution
OECD	Organization for Economic Co-operation and Development
OSCE	Organization for Security and Co-operation in Europe

PCI DSS	Payment Card Industry Data Security Standard
PKI	Public Key Infrastructure
PSD2	European Union Directive on Payments
SMEs	Small- and Medium-Sized Enterprises
TSP	Trust Service Provider
UGC	User-Generated Content
UK	United Kingdom
UNCITRAL	United Nations Commission on International Trade Law
UNGCP	United Nations Guidelines for Consumer Protection
U.S.	United States
US	United States
WTO	World Trade Organization

Glossary

Adequacy Approach: evaluation of the adequacy of a jurisdiction's laws and regulations (in this Guide used to refer to a basis for permitting ongoing cross-border data transfer in which regulators evaluate whether the domestic laws of the data exporting jurisdiction are adequate to protect the transfer)

Alternative Dispute Resolution: a mechanism for resolving disputes whereby the parties use techniques other than litigation to come to an agreement

Arbitration: a form of alternative dispute resolution where parties agree to designate an independent third party (a tribunal, comprised of one or more arbitrators) to resolve the dispute between them and agree to be bound by the decision

Automated Clearing House Payments: an electronic funds-transfer system

Bank-related E-payments: e-payments that are connected to banking systems through different types of bank accounts, such as debit cards, credit cards, and Automated Clearing House payments

Basic E-signatures: a type of e-signature whereby the signer applies their hand-signature to a document electronically and the document as a whole is protected with a cryptographic digital signature owned by a service provider organization that acts as a "witness" to the signing

Binding Corporate Rules Approach: a basis for permitting ongoing cross-border data transfer whereby regulators assess whether an enterprise's independent review mechanisms are sufficient

Click-to-sign Signatures: a type of e-signature that includes tick boxes, e-squiggles, scanned images, and typed names

Cryptocurrency: a digital or virtual currency that uses encryption techniques for security and generally operates without a central bank

Data Analytics: extensive use of data to improve predictions and support decision making

Data Localization Requirement: the requirement that businesses store data or a copy of data on servers that are physically located within national boundaries

Data Subjects: people whose personal data are being collected, held, or processed

Digital Signatures: the most advanced and secure type of signature, which uses a certificate-based digital ID issued by a Certification Authority or Trust Service Provider (TSP) that uniquely links the signature to the identity of the signer.

Ex ante Regulation: regulations that contain requirements for entering and operating in the market through either case-by-case regulatory approval or broader measures (in this Guide refers to regulation of non-bank related e-payments)

Ex post Regulation: regulations that apply once enterprises are operating in the market (in this Guide refers to regulation of non-bank related e-payments)

Extra-territoriality Clause: a legal provision that permits the application of domestic laws to overseas e-commerce enterprises

Forum Shopping: when a party to a dispute recognizes that multiple courts might have jurisdiction over the claim and chooses the one that would treat his or her claim most favorably

Jurisdiction: a country, state, or other area where a particular set of law or rules must be obeyed; jurisdictions may be countries or nations, sub-national entities, economic unions (for example, the European Union), or autonomous territories (for example, Hong Kong). Jurisdictions may overlap within a territory.

Laws (or Acts): legal measures, which often must go through a parliamentary process, that create a framework for governing the market and often relate to a particular sector or activity. Laws tend to be more general than regulations and create legally enforceable obligations.

Mediation: a form of alternative dispute resolution where an independent third party (mediator) uses persuasion rather than legal power to help bring about a resolution

Non-bank E-payments: e-payments that are not connected to banking systems

Non-prudential Regulations: financial regulations that apply to issues other than the stability of either the financial system or individual institutions s; covers all financial regulations that are not macro-prudential (related to the stability of the financial system) or micro-prudential (related to the stability of individual financial institutions)

Policies: principles or strategies that guide government actions (and may contain objectives for laws and regulations) but do not tend to be legally binding instruments on their own

Prescriptive Regulation (or Technology-specific Regulation): regulations that specify a certain method or technology; in this guide used to refer to e-signature regulations that legalize limited types of e-signatures

Prudential Regulation (or Micro-Prudential Regulation): financial regulations that relate to the stability of individual financial institutions

Public Key Infrastructure: a means of authentication and access control over untrusted networks such as open telecommunications network or the internet; typically used to verify digital signatures

Regulations: legal measures that are created, often through administrative action, to implement laws; tend to be both more detailed than laws or acts and also easier to change

Regulatory Sandbox: a legally safe space, monitored by regulators, for businesses to test new products, services, business models and delivery mechanisms without adverse legal repercussions

Regulatory Technology: a new category of businesses that use data analytics to help enterprises comply with regulations; primarily for compliance with financial regulations

Right of Access: data subjects' right to access their personal data and supplementary information

Right of Rectification: data subjects' right to have inaccurate or incomplete personal data be corrected or completed without undue delay

Right to Be Informed: data subjects' right to be informed about the collection and use of their personal data

Right to Data Portability: data subjects' right to obtain and reuse personal data for their own purposes across different services

Right to Erasure: data subjects' right to have their personal data erased

Right to Object: data subjects' right to object to direct marketing and processing

Right to Restriction of Processing: data subjects' right to request the restriction of suppression of their personal data

Right to Withdraw (or Cooling-off Period): a right of consumers to cancel an online order within a pre-determined window of time

Risk-based Approach: a cybersecurity monitoring strategy that requires public and private entities to conduct regular risk assessment exercises and monitoring processes, periodically evaluate the effectiveness of identified controls, and adjust their control mechanisms based on their evaluation.

Small Claims Courts: special judicial processes for handling claims under a specified monetary threshold that are generally faster and more cost-effective

Financial Regulation (or Macro-prudential Regulation): financial regulations that cover a range of measures designed to identify and mitigate risks to the stability of the financial system as a whole

Technology-neutral Regulation: regulations that apply regardless of the type of underlying technology; in this guide, the term refers to 1) e-signature regulations that apply equally to handwritten signatures and e-signatures (regardless of underlying authentication technologies) and 2) consumer protection laws and regulation that apply both in traditional and digital economy

The Referential: a means to streamline the dual certifications for data transfer under the European Union data transfer mechanisms and Asia-Pacific Economic Cooperation Cross-Border Privacy Rules

Trade Facilitation: the simplification, modernization, and harmonization of export and import processes for trade in goods

Two-tiered Regulation: e-signature regulations that recognize the legality and validity of multiple types of electronic signatures but give higher evidentiary value to digital signatures authenticated by certain technologies

Part II – Legal Deep Dives

Legal Deep Dive – Consumer Protection

Consumer protection law is central to all transactions, since it protects individuals and enterprises who purchase goods and services through electronic and non-electronic means. Consumer protection laws are meant to shield consumers from "improperly described, damaged, faulty, and dangerous goods and services as well as from unfair trade and credit practices."[1] Traditionally, legal frameworks for consumer protection have been designed to meet the needs of customers in an offline setting. However, consumer protection is doubly important in the digital economy. Adequate protections help cultivate a trustworthy environment so that both consumers and local businesses can engage confidently in online transactions. Currently, conventional consumer protection regimes are often not equipped to address practices particular to e-commerce, such as advertising on social media. As a result, there are gaps in consumer protection under most legal systems, and local business communities find their particular needs insufficiently addressed.

This deep dive into the legal and regulatory frameworks governing online consumer protection presents some illustrative examples of the different regulatory practices pertaining to the digital economy. It also addresses key considerations for both the local business community and regulators as more countries begin enacting and implementing consumer protection frameworks that specifically address digital consumer concerns. This deep dive begins with an overview of the international and regional frameworks already in place for consumer protection, which is a useful starting point for policy dialogues at the domestic level. It next outlines some common regulatory approaches to consumer protection, specific challenges related to regulatory implementation and enforcement, and examples of relevant institutional frameworks. In addition, the Consumer Protection section within the Summary Guide holds takeaways for business and advocacy guidance for the local business community, including a checklist for analyzing existing local consumer protection laws and regulations.

International and Regional Frameworks for Consumer Protection

International guidelines are helpful for identifying the rights and concerns of consumers and business. They are areas where new regulations or reforms to existing regulations may be needed. Second, an international framework could help encourage cooperation among governments, improve enforcement, and allow for collaborative exploration of ways to address common challenges in the sector. Importantly, regional initiatives contain more detailed provisions than those at the international level, and provide more specific intervention points for advocacy efforts. Table 1 lays out some illustrative current international and regional initiatives for consumer protection.

Table 1. International and Regional Frameworks for Consumer Protection

Initiatives	Implications for the Business Community
Multilateral	
• The Organization for Economic Co-operation and Development (OECD) Guidelines for Consumer Protection in E-commerce[2] • The United Nations Guideline for Consumer Protection (UNGCP)[3] • The United Nations Commission on International Trade Law (UNCITRAL) Model Law on E-Commerce[4] • The International Consumer Protection and Enforcement Network (ICPEN)[5]	• Overall, initiatives at the multilateral level promote cooperation and information exchange but they do not establish a unified international framework for consumer protection. This is a possible avenue for future engagement. While they may assist local business communities in the domestic policymaking context, the international frameworks are better detailed in other issue areas. • The OECD Guidelines cover consumer-to-consumer transactions (not just business-to-consumer), thus covering a wide range of stakeholders in the digital economy. The OECD Guidelines focus on cooperation and coordination among consumer protection enforcement authorities to improve the effectiveness of active investigations. • While the UNCITRAL Model Law mentions consumer protection, it does not contain country-specific obligations. It provides a more general view of how consumer protection fits within e-commerce. • The OECD, UNGCP, and ICPEN all facilitate or encourage multinational cooperation and information exchange. This eases the burden that falls on the business community to navigate overlapping regulations.

	• The ICPEN facilitates information exchange; publishes guidelines, which promote transparency; and serves as a complaint site for online scams. The business community could use this network as a neutral forum to resolve disputes, as well as a reliable source of information on consumer protection laws.
Regional	
• New Consumer Protection Cooperation (CPC) Framework (2017)[6] • European Consumer Centers Network (ECC-Net)[7] • The Association of Southeast Asian Nations (ASEAN) Strategic Action Plan for Consumer Protection (ASAPCP)[8] • Digital Agenda for Latin America and the Caribbean (eLAC2018)	• Regional initiatives focused on consumer protection all contain examples of good regulatory practices that could be adapted domestically. These channels could also be used to a greater extent by business groups within the relevant regions. • The CPC framework facilitates enforcement of regional consumer rules, specifically for cross-border transactions. • The ECC-Net serves as a regional advisory center for consumer protection rights and obligations. With built-in stakeholder support mechanisms for both the public and private sectors, like community town halls and stakeholder alignment meetings, ECC-Net serves as an avenue for advocacy at the European level. • The ASAPCP integrates ASEAN consumer protection policies and establishes a regional online dispute resolution (ODR) network. It forms an additional enforcement channel within ASEAN member states. • The eLAC2018 aims to adapt existing consumer protection regulations to the digital environment across the region. It also provides avenues for private sector participation in the decision-making process.

Regulatory Approaches to Consumer Protection

Consumer protection regulatory frameworks vary considerably country by country. Nevertheless, all such frameworks aim to strike a balance between the rights and responsibilities of all stakeholders in an electronic transaction. To better understand these legal rights and obligations, local businesses should first understand where the responsibilities lie for consumer protection. Responsibility tends to be allocated across regulators, consumers, and industry, particularly e-commerce platforms, and online vendors. Responsibilities are allocated differently at each stage of a transaction – pre-purchase, payment, and after sale or delivery. Understanding the rules at each stage will help advocates of the local business community make informed decisions on the trade-offs that exist within each regulatory approach.

In allocating responsibility, some countries (such as Chile and the US[9]) rely heavily on the judicial system. In these locations, the proper methods of dispute resolution are of the utmost importance. Other jurisdictions focus more on government regulation or business self-regulation; some work to empower consumers with information, so that they can make informed choices to drive the marketplace.[10] Public-private partnerships are a popular mechanism for feedback. In Spain, for instance, businesses can choose to voluntarily sign on and abide by Confianza Online's Ethical Code, targeting advertising, e-commerce transactions, and consumer redress mechanisms. This binds them to a certain standard of care, which is frequently updated to reflect the changes in the law.[11]

Other countries, like Malaysia, specifically regulate host businesses that operate through platform-based business models.[12]

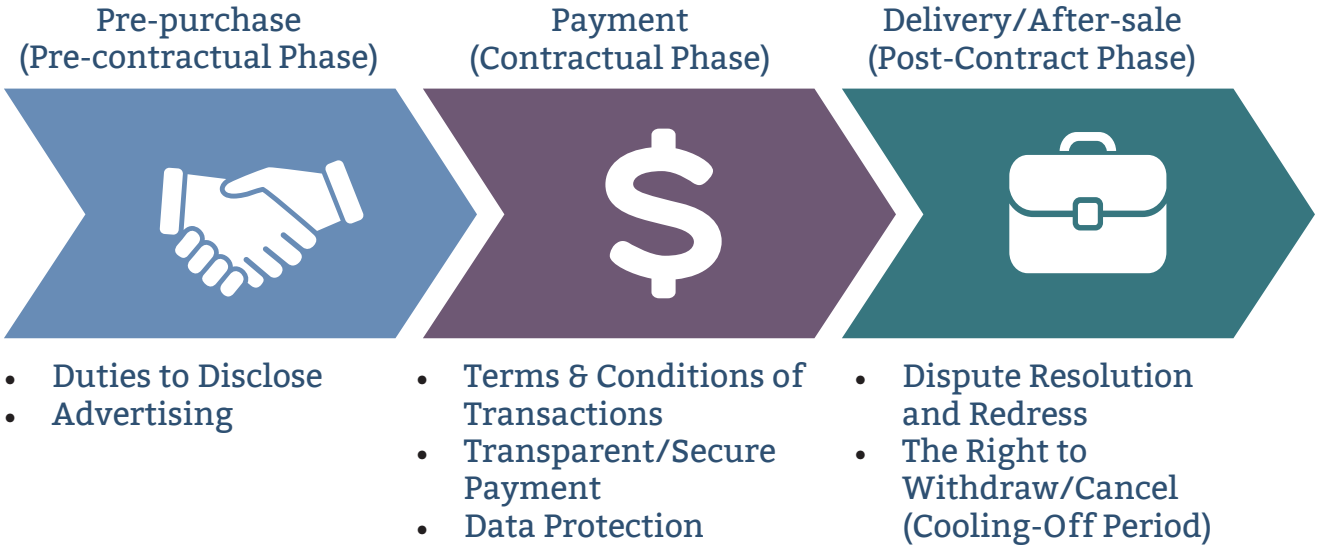
Many jurisdictions have consumer protection laws, regulations, or policies that apply to traditional offline transactions. Some choose to apply these same laws to the digital economy, as they address consumer needs that are present in both online and offline transactions. Others have chosen to create entirely new laws or regulations to address the special needs of the digital economy. A good example is South Korea's Act on Consumer Protection in Electronic Commerce.[13]

The local business community should always take care to identify any aspects of e-commerce that are not covered by the existing regulatory regime: counterfeit goods, for example, or advertising on social media.

Consumer protection regimes often share a few common elements. These common elements address consumer needs at different stages of a transaction, as set out in **Diagram 1**. (This Guide addresses two of those elements, data protection and transparent, authenticated online payments, in later chapters.) Local business communities stand to benefit from a protection regime that addresses issues throughout the different transactional stages; it builds trust in e-commerce, simplifies digital transactions, and engages more consumers online.

The remainder of this section illustrates the ways that various jurisdictions address each element of protecting consumers in a given transaction.

Diagram 1. Regulatory Elements of Consumer Protection



Source: New Markets Lab (2018)

Duties to Disclose: Many jurisdictions designate the types of information that online vendors must disclose so that consumers can make informed purchases. This information is usually classified as 1) **business information**, such as the trader's name and the address at which the trader is established, as required within the European Union (EU);[14] 2) **mandatory product labelling**, particularly for high risk products such as food; and 3) disclosure of governmental inspection results.[15]

Advocates for the local business community should be aware of the ways in which regulators allocate risk within their jurisdiction, and which obligations are placed on businesses as opposed to consumers.

Advertising: Advertisements are representations made by sellers to inform and attract consumers to a product or service. Consumer protection laws ensure that those representations are not misleading.[16] A major issue area here is whether conventional advertising regulations apply online. In many jurisdictions, like Japan,[17] existing advertising laws continue to apply in online marketplaces and are enforced by the same regulatory authorities. The rise of advertising on social media has also raised some interesting legal questions. Some jurisdictions have enacted regulations that reach well beyond traditional e-commerce providers. For example, the Advertising Standards Authority of Singapore issued guidelines that require marketers, including celebrities (or "influencers"), to fully disclose in simple language their relationships to brands when promoting or endorsing products through social media.[18] Another newly emerged tactic is user-generated content (UGC), including online consumer reviews and ratings on websites such as Yelp and TripAdvisor. Common legal issues that relate to UGC include intellectual property, data privacy, and consent.[19]

Terms & Conditions of Transactions: Like any transaction, digital sales carry certain terms and conditions, which have consumer protection implications. The most relevant aspects are 1) **disclosure and transparency**, and 2) **fair terms and conditions**. These go hand-in-hand since disclosure and transparency rules obligate traders to display terms and conditions that are "likely to affect a consumer's decision regarding a transaction."[20] The disclosure must also be accessible. For instance, in Argentina, traders need to provide clear, comprehensive, and unequivocal access to the general terms.[21] In practice, terms and conditions can be difficult for consumers to comprehend, which can undermine the intent. An analysis from the United Kingdom (UK) found that 43 percent of adults in England could not understand Google's 2013 terms and conditions.[22] However, few regulations mandate the use of clear and generally comprehensible language.

Businesses could follow the OECD's recommendation that online disclosure and its terms be made in "plain and easy-to-understand language."[23] The business community and regulators could also go a step further and advocate that disclosures be made in multiple local languages. Although this might place a greater burden on small and medium enterprises (SMEs) and startups, it would encourage diversity. "Fairness" is interpreted differently across jurisdictions. While some jurisdictions routinely uphold standard contracts between corporations and consumers, others (such as the EU) deem that a term that has not been individually negotiated (such as those that appear frequently in standard contracts) is unfair if it disrupts the balance between the parties' rights and obligations.[24] By advocating a more harmonized definition of fairness, local business communities can exercise their rights on this topic.

Dispute Resolution and Redress: Disputes between merchants and consumers come up routinely in e-commerce. There are various mechanisms to resolve these disputes, each with its own trade-offs and particularities. Traditional court systems are not always reliable. They are a notoriously difficult forum for consumers to enforce online rights due to court costs, limited access to adequate counsel, complications over jurisdictional limits, and prolonged litigation work that acts against the consumer's favor.[25] For e-commerce transactions, online dispute resolution (ODR), offered by public and private entities, can be a faster alternative to court.[26] Arbitration and mediation are also options.

The best choice in a given dispute will depend on the reliability of the local court system; availability of qualified and affordable arbitrators; confidentiality of judgments, usually preserved in arbitration; and the ability to appeal a decision (results of an arbitration panel can only be appealed under limited circumstances).[27] In the case of cross-jurisdictional contract disputes, arbitration tends to treat foreign parties with greater neutrality. Domestically, arbitration often works better than litigation in court,[28] although it can be expensive for consumers and small enterprises.

Working alongside the public sector to design fair and equitable dispute resolution mechanisms is a good way for the business community to protect its rights.

Right to Withdraw/Cancel (Cooling-Off Period): Because inspecting products before purchase is more difficult in e-commerce, consumers end up vulnerable to deceptive marketing. As a result, some regulators have stepped in to provide consumers with the right to cancel their orders, otherwise referred to as the right to withdraw or a cooling-off period. The length of this period varies: 14 days in the EU,[29] 7 days in China,[30] 5 days in Singapore, and 10 days in Malaysia.[31] Some regulators have also imposed a minimum price, below which the right to withdraw cannot be exercised. In the United States, for example, that price is $25 at the federal level. Some jurisdictions also include exceptions to the right to withdraw: personalized goods, perishable goods, or digital content are all exempt from right to withdraw rules.[32] Clear regulations on rights to withdraw could help protect both consumers and the local business community by reducing the numbers of disputes. This in turn could relieve the courts of some of their burden.

Implementation and Enforcement of Consumer Protection

As business transactions become increasingly international, enforcement remains local. Challenges exist for all stakeholders seeking proper enforcement of consumer protection laws. As with proper advertising and disclosure of terms and conditions, language and cultural differences complicate implementation and enforcement. What people understand in a local or regional market context will not necessarily translate in the global market. Even the translation of online platforms can cause problems, especially for industries without common standards and terminology. Not every company has the capacity to translate a webpage into the language of consumers, or fully anticipate consumers' needs. Furthermore, many consumers do not know where to lodge complaints in an international dispute.

For law enforcement and juridical processes, having parties agree on translations of a given document (like terms and conditions of transactions) can be costly and time-consuming. The degree to which law enforcement officials cooperate across jurisdictions can hamper good enforcement. Despite these challenges, there are ample opportunities for the local business community to become involved with efforts that would support better implementation of laws. The case study on ODR in Peru in the Summary Guide provides an example of cooperation between the public and private sectors to improve enforcement. It also demonstrates how the local business community can proactively work to solve some of these key regulatory challenges.[33]

Institutional Frameworks Related to Consumer Protection

As with enforcement and implementation, a main challenge within the institutional framework of consumer protection is clear designation of authority. In many jurisdictions, one central regulator or ministry, with broad legislative and oversight mandates, handles consumer protection.[34] This centralized approach can minimize overlapping regulatory mandates, keep policies consistent, and reduce potential conflicts between different agencies.[35] Examples of this approach include the Danish Consumer Ombudsman institution; the Ministry of Industry, Investment, Trade and Digital Economy in Morocco; and the National Consumer Commission in South Africa. Notably, due to the close link between competition policy and consumer protection,[36] some primary consumer protection regulators are also competition regulators.[37]

Some jurisdictions have adopted more of a sectoral approach, which could allow regulators to develop deeper expertise in their regulated industry and respond to industry-specific regulatory needs. Australia and Norway follow this model.[38] No matter the approach used, a shared key consideration for the local business community is clarity on what specific responsibilities and duties each regulator has.

Legal Deep Dive – Data Protection

Sometimes called the oil of the digital economy, data have become a key global commodity and are harnessed, processed, exchanged, and analyzed in massive quantities to power digitalized content, goods, and services. Data protection regulations relate to both individuals who purchase goods and services electronically and companies that buy, sell, or provide services online by protecting the data submitted in these transactions.

Regulation tends to follow the steps in the data lifecycle – data collection and processing, storage, transfer, and disposal. However, businesses may have different considerations in how data should be regulated, depending upon their specific business model.

This deep dive into the legal and regulatory frameworks governing data protection presents some illustrative examples of the different regulatory practices used across the world. It also addresses key considerations for both the local business community and regulators as more countries begin enacting and implementing data protection frameworks. The deep dive begins with an overview of the international and regional frameworks already in place. It then outlines some common regulatory approaches to data protection, including institutional frameworks and specific challenges related to implementation and enforcement. In addition, the Data Protection section within the Summary Guide contains further advocacy guidance for the local business community, including a checklist for analyzing existing local data protection laws and regulations.

International and Regional Frameworks for Data Protection

Legal frameworks for data protection differ country by country, making it difficult to understand the rules when working in multiple markets. Companies that rely on data imports or exports often face increased compliance costs or an inability to operate in certain markets. There are international initiatives to harmonize national frameworks underway; so far, these initiatives have only set out general principles.

Rules at the regional level tend to be clearer, but still suffer from a lack of overall harmonization. Regional communities have also begun working together to streamline rules on data protection. For example, the Asia Pacific Economic Cooperation (APEC) and the EU have already taken steps to streamline dual certifications, including the endorsement of a referential agreement in 2014.[39] This certification system has received support from regulators and businesses advocacy groups alike (see the case study below). While it is uncertain whether and when this program will officially take off, it seems that APEC certification will expedite and lower the cost of certification under EU Binding Corporate Rules (EU BCR).[40] This effort to link regional systems might prove a good model for cross-regional collaboration.

Local business communities can actively call on governments to facilitate cross-border flow of data. This can be done through a coalition of business associations in different jurisdictions, as exemplified by the expansion of APEC's Cross Border Privacy Rules (CBPRs). The APEC Privacy Framework was created to promote a common set of data protection rules and standards to facilitate cross-border data transfer throughout Asia and the Pacific. It lays down a single framework of principles and implementation guidelines (for example, security safeguards) and allows its 21 members to adopt the Privacy Framework, with flexibility in how to do so. Companies working in APEC countries can be proactive and certify that they are in compliance with the APEC Privacy Framework by adopting the APEC Cross-Border Privacy Rules (APEC CBPRs), endorsed by APEC leaders in 2011. APEC CBPRs are voluntary yet enforceable rules for cross-border data transfer, and widely supported by the business community. APEC CBPRs can be particularly helpful to local enterprises that rely on cross-border data transfer, but which do not have the resources to formulate their own privacy programs; as is the case in the Association of Southeast Asian Nations (ASEAN) economies, where SMEs comprise 96 percent of all businesses.

In late 2016, eight major business groups representing hundreds of businesses around the global jointly released a statement voicing their support of the CBPR system, and that called on 21 APEC members to increase participation in CBPRs for both member states and the private sector. This advocacy has had an impact, as now six economies are participating in the CBPRs program with more expected to join.

Case Study:
Asia-Pacific Economic Cooperation (APEC) Privacy Framework

Trade agreements also strengthen the link between international trade and digital economy issues, including data protection.[41] In contrast to privacy-specific initiatives, trade agreements do not impose significant positive obligations. Instead, they aim to create a balance between data protection laws and trade considerations. The US has advocated for this approach, and it is fast becoming the standard, as evidenced by the US-South Korea Free Trade Agreement, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (the follow-on agreement to the Trans-Pacific Partnership),[42] and the recently concluded Singapore-Sri Lanka Free Trade Agreement.[43] Including data provisions within trade agreements could limit the degree to which individual nations can address data protection, and may require governments to balance a broad, unwieldy range of policy areas, such as environmental protection and tariff reduction. **Table 2** below summarizes the major global, regional, and bilateral instruments applicable to data protection.

Source: CPBRs, About the APEC CBPR System. Web; ITI, Global Industry Groups Call for APEC Leadership on Facilitating Cross-Border Flows of Information with High Standards of Privacy Protection. Web. November 18, 2016.

Table 2. International and Regional Frameworks for Data Protection

Framework	Implications for the Business Community
Multilateral	
• The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[44] • Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data[45]	• The OECD Guidelines provide eight privacy principles and concepts with broad international support (for example, risk assessment and improved interoperability). They are an excellent resource for local business communities and regulators alike.
Regional	
• CPTPP[46] • APEC[47] • African Union Convention on Cyber-security and Personal Data Protection[48] • Economic Community of West African States (ECOWAS) Supplementary Act on Data Protection[49] • North America Free Trade Agreement (NAFTA) (under renegotiation)[50]	• Regional data protection frameworks all highlight illustrative regulatory positions and details of their provisions. These channels could also be used to a greater extent by business groups within the relevant regions. • All the regional agreements on this list address data protection specifically. • APEC, for example, allows companies to obtain certification to demonstrate compliance with the APEC Privacy Framework through a voluntary mechanism, serving as a good practice for stronger self-regulation. It also establishes principles and implementation guidelines to facilitate transfer of data and harmonized approaches among APEC members.
Bilateral	
• US-South Korea Free Trade Agreement[51]	• Bilateral trade agreements are beginning to contain provisions related directly to electronic information flows, as this example highlights, which could inform positions taken by the business community domestically and with respect to future agreements.

Regulatory Approaches to Data Protection

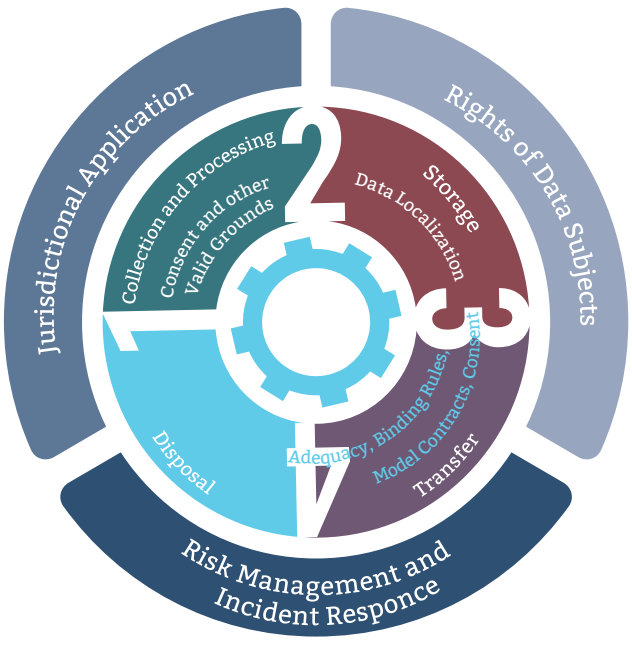
At the domestic level, the local business community should pay special attention to data protection regimes. Many countries are currently passing laws and regulations in this area; taking stock of relevant rules will help business advocacy groups work with policymakers and other stakeholders to enact the most suitable approach. Businesses can also use robust data protection systems to boost brand reputation, which builds trust with consumers and users. While data protection regimes are often complex, the key themes discussed below will help guide the local business community as they navigate this still-emerging area of law.

Different jurisdictions regulate data protection very differently, in terms of both scope and focus of regulations. Some, like Japan, Ghana, and the EU, have adopted comprehensive regulations that cover all activities involving data under a single legal instrument. Others, like the US, regulate sector by sector.[52] South Korea is also an example of the latter, with different laws applying to information technology (IT), financial transactions, and the disclosure of personal credit information.[53] While Brazil currently takes a similar sectoral approach, two draft laws under consideration would move the country toward one broad data protection framework.[54] Regulations may also differentiate based on sensitivity of data (as in the EU and Russia, where more stringent requirements apply to sensitive data); the capacity and data impact of entities (in Australia, businesses with an annual turnover of AU$3 million or less are not subject to the Privacy Act);[55] or special categories of people (for example, children – the Child Rights Act No. 26 of 2003 in Nigeria protects the privacy of children under 18).

Finally, some jurisdictions with influential data protection regimes, such as the EU's General Data Protection Regime (GDPR), are more consumer-centric, granting a range of rights and power to consumers.[56]

In practice, data protection regimes can include a mix of policy instruments, such as constitutional provisions, laws, regulations, and standards.[57] Regardless of the legal instruments, common regulatory elements include both obligations governing steps in the data lifecycle (collection and processing, storage, transfer, and disposal) as well as cross-cutting obligations (responses to a data breach, the application of domestic laws to overseas enterprises, and rights of individuals whom data are about).[58] These regulatory elements are mapped in **Diagram 2** and explained in detail below.

Diagram 2. Regulatory Elements of Data Protection Regimes



Source: New Markets Lab (2018)

Regulatory Approaches that Apply at Different Stages of the Data Lifecycle

Collection and Processing: In many jurisdictions, companies that collect and process data in the course of their business operations must have valid grounds for doing so, including the consent of the data subjects. As of early 2018, Egypt was close to finalizing a draft law that would incorporate a consent requirement and general data protection rules into the Egyptian constitution.[59] Other countries are moving in that direction as well.

Storage: Many jurisdictions require that businesses store data on servers that are physically located within their national boundaries. These rules are called data localization requirements. Examples include Germany, Kyrgyzstan, Nigeria, Indonesia, Russia, Greece, China, Malaysia, and Australia.[60] Many enterprises, particularly those working in more than one country, report that data localization requirements are financially burdensome and can divert already limited financial resources. For local business, these requirements can discourage business operations that rely on international data flows. In 2013, for example, building data centers in Brazil and Chile was estimated to cost US $60.3 million and US $43 million, respectively.[61] As discussed below, some international trade agreements now include provisions to curb data localization requirements, and the business community can focus advocacy efforts to support this trend.

Data Transfer: Jurisdictions restrict cross-border data transfer to varying degrees. Transfers may sometimes be permitted under one-time or ongoing exceptions. One-time exceptions (for example, for the fulfillment of contracts) are common.[62] However, ongoing exceptions are treated very differently case by case, and often require an assessment of whether there is a sufficient degree of data protection. Ongoing data transfers are typically handled by data receiving jurisdictions under one of the following four approaches, with differing implications for the local business community and data exporting governments:

1. Evaluation of whether the domestic laws of the data-exporting jurisdiction are adequate: the adequacy approach, which places the burden on the public sector;
2. Assessment of whether the independent review mechanisms of a given enterprise are sufficient, like the EU and Japanese Binding Corporate Rules (BCR) systems and the and APEC Cross-Border Privacy Rules (APEC CBPRs): the corporate binding rules approach, which places the burden on the private sector;
3. Evaluation based on contractual protections: the model contracts approach, rarely used; or
4. Assessment of individual consent to the data transfer: the consent approach, which places the burden on the private sector to show consent.[63]

Among these, the first two approaches are the most widely followed, although their application may differ by jurisdiction. Stakeholders based in a jurisdiction with weak data protection laws may prefer the corporate binding rules approach. The model contracts approach might also be an option but is used much less frequently (to date, only in the EU) and depends upon full implementation of model contracts.[64] On the other hand, stakeholders located in a jurisdiction with strong data protection rules could request that their government seek "adequacy status" from another jurisdiction, which would streamline data transfer overall. The strengths and weaknesses of each approach are included in **Table 3**.

Disposal: Once data have fulfilled their intended purposes (for example, when a transaction is completed), some jurisdictions require the destruction or disposal of the data. In such jurisdictions, the local business community would need to carefully monitor a wide range of hardware and software used for data storage to ensure complete disposal of all relevant data. Enterprises may also need to designate or hire records retention managers to ensure complete and secure disposal, especially for data that are stored in cloud services.[65] Business advocacy groups should consider the different burdens placed on the local business community under different disposal laws, and support approaches that best suit the needs of both SMEs and larger firms.

Table 3. Approaches for Managing Cross-Border Data Transfer

Approach	Strengths	Limitations
Adequacy	• Enables comprehensive transfer (for those jurisdictions found adequate) • Promotes interoperability and harmonization • Transparent and open "whitelist"	• Causes significant difficulty for jurisdictions not found adequate • Struggles to accommodate jurisdictions with different approaches to data protection • Lengthy process to determine adequacy
Binding Corporate Rules	• Enables free movement of data within a corporate group • Promotes best practices data protection processes and oversight in the private sector • Transparent and open list of participating countries	• Lengthy and expensive approval process • Limited use for other data transfers outside the corporate group

Model Contracts	• Promotes interoperability and harmonization • Can be quickly implemented by individual businesses willing to adopt the model contracts clause verbatim	• Challenging to develop appropriate model clauses and to keep them up to date • No transparency about who is using model clauses • Limited opportunity for oversight
Consent	• Quick and easy solution for certain types of transactions • No detailed analysis or review required • Low compliance burden for businesses	• Unsuitable for many contemporary transactions • Open to differing interpretations of consent, and prone to complaints and disputes • Potential for lack of fairness in situations where there is a significant power imbalance between the parties • Potential to promote fragmentation rather than harmonization of data protection practices

Source: Data Protection Regulations and International Data Flows: Implications for Trade and Development. 14. United Nations Conference on Trade and Development. Web. 2016 (modified by New Markets Lab, 2018).

Overarching Regulatory Approaches

While the regulatory considerations above are specific to different stages in the data lifecycle, the issues below apply across the lifecycle and can have a broader reach.

Registration and Notification: Many businesses engaged throughout the data lifecycle are required to register with the domestic regulatory body, or provide notification of activities. While there is variation in these requirements, they can be a particular challenge for SMEs and startups. One type of requirement involves notifying local data protection authorities of relevant businesses or datasets.[66] In Ghana, data controllers and processors must notify the Data Protection Commission of everything from the type of data an enterprise holds to the nature of processing that the enterprise undertakes.[67] As in other countries, the fees can be substantial: in Ghana they often amount to 750 Ghanaian cedis, or US $167.

To lighten compliance burdens for local business, lawmakers could draft regulations with different tiers based on firm revenue or include other built-in exemptions, similar to the exceptions under Australia's Privacy Act based on firm revenue.[68] Regulatory commitments may also be applied incrementally based on capability. This could include longer grace periods for implementing certain obligations for enterprises under a given size.

In some cases, third-party certification schemes are taking the place of formal government registration. These include the binding corporate rules approach (the European BCR and APEC CBPRs). This approach entails fees such as application payments to the scheme operator, and third-party certification services for annual certification. The downside of this approach is the time it takes (an average of 18 months for obtaining the EU certification); otherwise, it is much more streamlined.

Responses to Data Breach: To build a system that can withstand and minimize the impact of data breaches, many jurisdictions have imposed obligations regarding risk management and incident response. Regulations tend to cover organizational, monitoring, and incident response measures. At the organizational level, some countries, such as the EU, China, Mexico, and the Philippines, require the establishment or appointment of dedicated data protection officers (DPOs). More stringent requirements may apply to some organizations (like those whose core business revolves around the large-scale processing of sensitive personal data), and DPOs may be required to possess "expert knowledge" of data protection laws.[69] Experienced data protection professionals are in short supply, and some enterprises may need to outsource the DPO role to an external provider, at great expense.[70]

Monitoring: Effective monitoring is critical to detecting potential data breaches early on. Some jurisdictions have adopted a risk-based approach, undertaking risk mitigation measures tailored to level of exposure. Mexico, for instance, requires companies to carry out security risk analysis.[71]

Incident response: This encompasses the actions governments or enterprises will need to take in the event of a data breach. Some jurisdictions have mandated notification, including Mexico[72] and the US.[73] The requirements vary in their specificity and coverage but generally include the following components: 1) **who must comply with the law, such as businesses or public entities**; 2) **coverage of the information**; 3) **definition of a data breach**; 4) **requirements for notice**, like timing or method of notice; and 5) **exemptions**, such as encrypted information.[74]

Rights of Data Subjects: Data subjects are the individuals who possess the personal data in use. Governments sometimes step in to provide a range of rights for data subjects, such as consumers, who generally do not have sufficient bargaining power to shape company policies. As noted above, some of the more influential data protection regimes, especially the EU's GDPR[75] (see **Diagram 3**) take a consumer-centric approach to data protection and grant far-reaching rights to consumers. GDPR has also been a model for jurisdictions looking to centralize their enforcement mechanisms and data protection frameworks, both discussed in further detail below.

Diagram 3: Rights of Data Subjects in the EU's GDPR.

Right to Be Informed	Right of Access	Right of Rectification	Right to Erasure ("Right to Be Forgotten")
Right to be informed about the collection and use of data subjects' personal data	Right to access data subjects' personal data and supplementary information	Right to have inaccurate or incomplete personal data to be corrected or completed without undue delay	Right for data subjects to have personal data erased
Right to request the restriction or suppression of data subjects' personal data	Right to obtain and reuse personal data for data subjects' own purposes across different services	Right to object to direct marketing and processing in limited circumstances	Right not to be subject to automated decision making, including profiling
Right to Restriction of Processing	**Right to Data Portability**	**Right to Object**	**Automated Decision Taking**

Source: New Markets Lab (2018).

Some rights can stimulate market competition, including among SMEs. For instance, a draft bill in Brazil[76] allows data stakeholders to request data portability: that is, that a copy of their data be directly transmitted from one controller to another. Smooth transmission of data, made possible by interoperability between different websites and platforms, could encourage new market entrants and increase competition in the service of potential clients who are otherwise unwilling to re-input all their data.[77]

Jurisdictional Reach: There is a growing trend among regulators to apply domestic laws to all foreign e-commerce enterprises that engage with domestic residents, a practice called extra-territorial reach. This could further increase compliance costs for businesses.[78] In Japan, the data protection law expressly applies to foreign entities that collect or have collected personal information of anyone residing in Japan.[79]

The local business community has to consider a range of laws, regulations, and other measures that govern data protection, depending on where the data subjects involved reside and the relevant stages in the data lifecycle with which they are involved. Additionally, business advocacy groups could press for a unified approach to cross-border data transfer and greater international harmonization.

Implementation and Enforcement of Data Protection

Enforcing data protection is an ongoing challenge. Two particular aspects of enforcement stand out, heavy sanctions and the right for private actors to claim compensation. For regulators contemplating heavy sanctions, as well as the local business community under such a regime, it is important to recognize the potential drawbacks. For instance, breach of a data protection laws in the EU could lead to revenue-based fines of up to four percent of annual global turnover, or criminal sanctions in countries like Japan, the Philippines, and Mexico.[80] While heavy sanctions could encourage companies to comply with data protection laws, they could also lead to "forum shopping,"[81] thus negating the deterrence effect of heavy fines. These measures also disproportionately affect SMEs, who do not have the same capacity as multinational companies to adjust terms of service in response to a change in the law. In other cases, enforcement officials (like those in China) may themselves perceive the fines to be too hefty and apply less stringent alternatives instead, such as administrative warnings.

Sanctions aside, some jurisdictions allow consumers to bring private claims. A case in point is Ghana's Data Protection Act. The Act establishes an independent statutory body to investigate complaints, and expressly provides for the "Right to Seek Compensation through the Courts" as part of data subjects' rights.[82]

Compliance with data protection regimes can be costly and cumbersome for the local business community overall. A report by the OECD highlighted that multinational companies spend over US $1 million in data-related compliance costs.[83] For all other enterprises, keeping abreast of with a mix of evolving global and national regulations, to say nothing of complying with those regulations, can be especially cumbersome. Three requirements, routinely present in national regulatory frameworks, have been identified as particularly burdensome for smaller businesses: 1) r**equirements to appoint data protection officers**; 2) **data localization requirements**; and 3) **registration requirements**.

For governments, enforcing data protection laws can be challenging due to capacity constraints and lack of awareness. Awareness-building campaigns could help create incentives for businesses to comply, and would certainly cost less than enforcement actions.[84] Both the enforcement challenge and the need for legal and judicial capacity building have been highlighted by the Commission on Human Rights and Administrative Justice in Ghana.[85] Even though the Commission has received some complaints about data breaches, enforcement actions under the Act have not been actively enforced. Those actions require further awareness and capacity among stakeholders, including prosecutors and judges. to effectively enforce applicable sanctions.

Institutional Frameworks Related to Data Protection

The institutional frameworks governing data privacy will play a central role in both how the sector is governed and how the local business community can engage with policymakers and other stakeholders. Where institutional frameworks for data protection vary from jurisdiction to jurisdiction, public or private channels may be available for advocacy and regulatory input. Some countries allow citizens and members of the business community to comment on proposed laws, including those that aim to regulate data protection. Actively providing input in the rulemaking process allows stakeholders to shape frameworks that respond to their needs. Panama is a case in point for participation in the legislative process, as elaborated in the Summary Guide.

At the national level, many countries are working to establish a single central regulator for data protection, with broad legislative and oversight responsibilities.[86] This approach streamlines compliance obligations for companies, provides a single point of contact for consumers seeking information or redress, and sets standards to minimize regulatory fragmentation, both at home and overseas.[87] These central regulators have released clear guidelines, conducted capacity building with businesses, and provided a single point of contact for stakeholder complaints. Other jurisdictions split regulatory roles by sectors or functions. South Korea, for example, divides regulatory and complaint management functions between two agencies.[88]

Case Study:
Public Commenting on Panama's Data Protection Act

Business associations can actively participate in the legislative process for data protection laws. Even though the process itself varies considerably across jurisdictions, administrative processes sometimes allow for engagement and comments from civil society and private actors. One example is the development of data protection legislation in Panama.

In mid-2016, the Panamanian Congress presented a bill regulating data protection in the country. It held a three-month-long public hearing to receive comments from civil society actors, private citizens, and businesses. The public hearing was conducted by the Innovation National Authority (Autoridad Nacional para la Innovación Guvernamental in Spanish) and the Transparency Agency (Autoridad Nacional de Transparencia y Acceso a la Información in Spanish) and had the special participation of the Organization of the American States and the Interamerican Court of Human Rights, meaning that regional and international frameworks were considered. Participants provided comments, which were included in the final bill presented to Panama's Congress early in February 2017. To promote public discussion on the matter, different organizations held conferences with a large private sector representative (Google) and the Panamanian Chamber of Commerce.

As of September 2018, the bill has not yet been adopted into law due to budgetary constraints. Nevertheless, the rulemaking process in Panama highlights a good practice of welcoming interested business associations to take part in the rulemaking process and voice their concerns. Regional and international institutions were involved as well. Similarly, in India, a Data Protection Bill was open for public comment until September 10, 2018.

Sources: IPANDETEC, Cronología de un Proyecto de Ley de Protección de Datos en Panamá, Jan. 29, 2018. Web; AIG, Consulta pública sobre Proyecto de Ley de Protección de Datos de Carácter Personal" refuerza el marco legal para la Economía y el Gobierno Digital, Jul. 11, 2016. Web; Violeta Villar, Panamá necesita aprobar Ley de Protección de Datos, El Capital, Feb. 14, 2018. Web; Gobierno de Panamá, Avalan proyecto que establece la protección de datos de carácter personal, Consejo de Gabinete, Jan. 18, 2017. Web.

Legal Deep Dive – Cybersecurity

Cybersecurity regulation, which protects information technology and computer systems from attack, is a major concern for the global business community, among other stakeholders. Recent attacks on computers and information networks, both public and private, have grown in scale and severity, to the dismay of governments, industry, and consumers. Cybersecurity broadly includes the assets of both public and private actors and covers "connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information."[89]

This deep dive into the legal and regulatory frameworks governing cybersecurity law will illustrate the different regulatory practices used across the world. It also addresses key considerations for both the local business community and regulators. This deep dive begins with an overview of the international and regional cybersecurity frameworks. It then outlines some common regulatory approaches to cybersecurity, specific challenges related to implementation and enforcement of laws and regulations, and examples of relevant institutional frameworks. In addition, the Cybersecurity section within the Summary Guide contains further advocacy guidance for the local business community, including a checklist for analyzing existing local cybersecurity laws and regulations.

International Framework for Cybersecurity

All countries regulate cybersecurity differently, and there is not yet a binding set of international rules designed to harmonize national systems. International frameworks, which include conventions, initiatives, and trade agreements, tend to center around international cooperation and capacity building. Generally, they are neither detailed nor prescriptive. Still, because they focus on capacity building and cooperation, they serve as useful tools and can help guide policy discussions. **Table 4** summarizes the key international frameworks relating to cybersecurity.

Table 4. International and Regional Frameworks for Cybersecurity

Framework	Key Implications for the Business Community
Multilateral	
• Budapest Convention • World Trade Organization (WTO) General Agreement on Trade and Services (GATS Agreement) • United Nations Office on Drugs and Crime/International Telecommunications Union (ITU) Memorandum[90]	• The Budapest Convention boosts international cooperation and global policy-making in combatting cybercrime. It harmonizes domestic criminal laws concerning cybercrime and provides guidelines for enacting domestic criminal procedures. Not only does it help establish an international standard, but it can also provide guidance for domestic discussions between the business community and policymakers regarding new laws, regulations, and policies. • The GATS requires non-discriminatory treatment and transparency once a country has made commitments to open domestic sectors to international trade. Business communities within WTO member states can use this as a rationale for increased transparency in rulemaking and enforcement. • The UN ITU Memorandum offers technical assistance and legal training for law enforcement officials and other stakeholders. The organization also seeks expertise from industry members, creating a channel for engagement.

Regional	
• Organization for Security and Co-operation in Europe (OSCE)[91] • International Code of Conduct for Information Security • Organization of American States (OAS) – Comprehensive Inter-American Cybersecurity Strategy[92] • The OECD Guidelines for the Security of Information Systems and Networks[93] • CPTPP	• Regional frameworks for cybersecurity all contain example regulatory positions that could inform positions taken by the business community domestically and with respect to future agreements. • The OSCE creates confidence-building measures and encourages member states to increase public-private cooperation (however, this provision is voluntary). • The International Code of Conduct for Information Security mandates that states "cooperate fully" with interested parties, including the private sector and civil society to improve the culture surrounding information security. This call for cooperation with the private sector could provide a channel for engagement. • The OAS Strategy develops a regional warning network to alert and inform about incidents across OAS Members and shares secure infrastructure for managing Computer Security Incident Response Team (CSIRT) communications with the private sector and other stakeholders. • The OECD Guidelines for the Security of Information Systems and Networks are a result of a multi-stakeholder initiative to modernize an older set of OECD guidelines. This collaborative approach resulted in comprehensive guidelines for national cybersecurity strategies. • The CPTPP contains provisions encouraging collaboration among signatories to assist SMEs in overcoming obstacles to e-commerce. While not a binding obligation, his could be an important advocacy channel in CPTPP countries.

Source: New Markets Lab (2018).

Regulatory Approaches to Cybersecurity

Despite these international and regional efforts, there is considerable variation in how jurisdictions regulate cybersecurity. Regulatory approaches have evolved in three waves over time. The first wave of regulation focused on cybercrime legislation, a top-down approach that starts with regulators and government action. The second phase involved private-sector led, multi-stakeholder enforcement of cyberlaw norms and standards. This wave began after the global financial crisis of 2008. The third phase consists of the more comprehensive cybersecurity legislation, which has become common in recent years. **Diagram 3** portrays the three phases of cybersecurity regulations, which will be addressed in greater detail below.

Diagram 3. Evolution of Cybersecurity Regulations

Cybercrime Legislation

First type of cybersecurity regulation adopted in most through a top-down approach. Most common cybercrimes include:

- E-Mail Spoofing
- Phishing
- Spamming
- Cyber-Defamation
- Cyber Stalking
- Identity Theft
- Software Piracy
- Unauthorized Access
- Denial of Service
- Web Defacing
- Ransomware
- Salami Attack
- Logic Bomb
- Data Diddling

Private Sector Led Multi-Stakeholder Enforcement

Private development of cybersecurity program, procedures, and standards is institutionalized through a multi-stakeholder framework

Comprehensive Cybersecurity Regulation

Recently enacted overarching regulations address:

- Coverage (general or sector specific)
- The preventive aspect (strategic, organizational, and monitoring mechanisms), and
- The reactive aspect (definition of cyber incident or cyberattack and legal obligations triggered by cyber incident or cyberattack)

Source: New Markets Lab (2018)

Jurisdictions tend to fall into one of these three phases. As the legal and regulatory framework continues to change, the business community may have different advocacy needs, depending upon where in the cycle their jurisdiction falls. The particular nuances of each of these phases are outlined below.

Cybercrime Legislation

Diagram 4. Common Types of Cybercrimes

Types of Cybercrimes	Phishing	Spamming	Cyber-Defamation	Cyberstalking
	The act of attempting to fraudulently acquire through deception sensitive personal information such as passwords and credit card details by assuming another's identity in an official-looking email, IM, etc.	Unsolicited commercial advertisements sent by email over the Internet. There is legislation addressing spam in at least 33 countries, including the EU.	False and unprivileged statement of fact that is harmful to someone's reputation and published "with fault", meaning as a result of negligence or malice.	Using the Internet, email, or other types of electronic communications to stalk, harass, or threaten another person.
Unauthorized Access/Hacking	**Denial of Service**	**Website Defacing**	**Ransomware**	**Salami Attack**
Approaching, trespassing within, communicating with, storing data in, retrieving data from, or otherwise intercepting and changing computer resources without consent, including hacking, malware and virus attacks.	When an attacker floods the bandwidth or resources of a targeted system or servers with traffic, thereby preventing legitimate users from accessing information or services.	Taking control of a web site fraudulently to either change the content of the original site or redirect the user to another fake similar looking page controlled fraudulently controlling by other.	Form of malicious software that infiltrates computer systems or networks and uses tools like encryption to deny access or hold data "hostage" until the victim pays a ransom, frequently demanding payment in Bitcoin.	Cyber crime usually used for the purpose of committing financial crimes in which criminals steal money or resources a bit at a time from financial accounts on a system.
Software Piracy	**Identity Theft**	**Logic Bomb**	**Data Diddling**	**E-Mail Spoofing**
The unauthorized copying/distribution of software.	Wrongfully obtaining and using another person's personal data in some way that involves fraud or deceprion, typically for economic gain.	Programming code that is hidden in a program or system that causes something to happen when the user performs a certain action or when certain conditions are met.	Unauthorized changing of data before or during their input to a computer system. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements.	Manipulating commercial email to falsify the email's true origin, without the consent or authorization of the user whose email addressed is spoofed.

Source: New Markets Lab (2018).

Early cybersecurity legislation focused predominantly on preventing a range of cybercrimes. **Diagram 4** above contains examples of the most common types of cybercrimes. Jurisdictions regulate cybercrimes to this day, and they remain an important part of overall safety online.

Cybercrime legislation will never be fully effective without sufficient sanctions and enforcement capacity. For example, in 2012 Brazil passed its first cybercrime law, which was accompanied by light sanctions like house arrest, and enforced by understaffed and underfunded cybercrime divisions.[94] Despite the enactment of this law, in 2017 Brazil was still ranked as the country with the most victims of cybercrimes in Latin America, with malware and online fraud as the primary crimes.[95]

Private Sector Led Multi-Stakeholder Enforcement

In addition to cybercrime legislation, enforcement led by the private sector helps guide businesses looking to establish preventive systems against possible cybersecurity risks. This approach harmonizes industry best practices (programs, guidelines, and standards) and adapts them to a framework comprised of government, industry, academia and international partners.[96] For enterprises, aligning with these practices could help prioritize investment in cybersecurity. Many of these guidelines allow flexible adoption, tailored to the size and nature of the enterprise.[97]

It is crucial for the local business community to keep abreast of these practices. Although these frameworks are voluntary, non-compliance with widely adopted best practices could put enterprises at a competitive disadvantage. Perhaps more importantly, this is a way for businesses to become involved in the lawmaking process early on and engage in public-private dialogue on best practices.

The UK has incorporated voluntary adoption of security guidelines into its 2011 UK Cyber Security Strategy.[98] An interesting feature of this strategy is the Cyber Essentials certification program, which creates incentives for the adoption of basic security controls. This program is mandatory for UK government contractors handling personal information.[99] The UK government, through Advice Sheets on the 10 Steps to Cybersecurity Program, facilitates the process by which companies of any size might obtain Cyber Essentials certification. Such accessible measures are particularly beneficial to SMEs, which can use the certification as a way of enhancing consumer confidence in products and services.[100]

Comprehensive Cybersecurity Legislation

To complement cybercrime and multi-stakeholder frameworks, many jurisdictions have rolled out new, comprehensive cybersecurity legislation. Under these frameworks, enterprises are frequently required to have certain systems, technologies, or plans in place to protect security online. Those that are involved in critical infrastructures, such as electricity grids, may be subject to additional requirements for national security purposes. It is worth noting here that an overly restrictive approach, such as those used in Russia, China, and Vietnam, could negatively impact the flow of information, with significant implications for international trade and freedom of expression.[101]

These comprehensive frameworks often have more stringent requirements related to post-cyber incident reporting. This differs from those regulations that use a result-oriented approach. This approach considers an event to be a cyber incident when the information system is actually breached. This approach is in effect in Russia.[102] Another method focuses on the attempt to breach, which is enough to constitute a cyber incident in itself. The US[103] and Singapore[104] adhere to this model. When determining which approach to advocate, the local business community should consider whether they can adequately comply with and respond to a more expansive approach. If this would be overly burdensome, the result-oriented approach might be a better option.

Reporting and other mitigation procedures are also common aspects of a comprehensive regulatory approach. Provisions do not always mandate prompt and detailed notifications. For instance, the US federal government does not mandate incident reporting,[105] whereas Russia requires banks to inform the Central Bank of any cyber-incident that threatens data security in payment transactions.[106] The EU is even more prescriptive and granular in its approach. In the EU, legislation has evolved to mandate incident reporting only for some sectors, such as the telecom industry and for digital service providers.

Implementation and Enforcement of Cybersecurity

As critical as a robust, resilient cybersecurity system is to both public and private actors, it can also pose a challenge. Regulators may find it difficult to keep up with changes in relevant technology and their applications. Even when cybersecurity legal and regulatory frameworks are in place, difficulties still arise with implementation and enforcement. SMEs, often the primary victims of cyber-attacks, face an array of challenges to meet mandatory regulations and voluntary industry standards. A study by the Ponemon Institute

in 2017 found that cyber-attacks affecting SMEs had increased from 55 to 61 percent in the span of a year.[107] A majority of these attacks were phishing or social engineering. Despite the prevalence of cyber-attacks, several key policy issues interfere with the adoption of cybersecurity measures by SMEs. These should serve as wedge issues for the local business community to engage with the public and policymakers.

The first issue is under-investment in cybersecurity. For instance, most Singaporean SMEs spend well below one percent of their revenue on cybersecurity, the figure deemed by the World Economic Forum to be the industry average necessary for all information and communications technology (ICT) industries to combat cybercrime. This underinvestment is perhaps caused by SMEs' misconception that cyber threats only affect large organizations or information and communication technology (ICT) companies. For example, a report by Juniper Research showed that 74 percent of SMEs in the UK think they are safe from cyber-attacks, even when they admit to having suffered from data breaches.[108]

In the private sector, insufficient room in the budget for combatting cybersecurity is another leading cause of underinvestment by SMEs.[109] It can be costly for SMEs to invest in the hardware, software, and organizational transformation needed to implement relevant regulations and standards. The baseline amount required for minimum protection[110] can easily exceed an SME's budget, which is often pegged to revenue or ICT spending.[111] Further, SMEs typically lack in-house personnel. This not only causes difficulty in adequately protecting computer systems, but also an inability to appropriately interpret technical standards or update software in a timely manner.[112] This practical difficulty is exacerbated by the fact that many of the technical standards lack implementation guidelines, making it difficult for SMEs to comply independently.[113] Common implementation guidelines could be developed by both larger enterprises and SMEs, which would ease the burden on SMEs.

At a systemic level, one of the reasons for inaccessibility is the fact that standards have been developed for larger organizations, which tend to have larger budgets and dedicated cybersecurity and advocacy teams. There is a sense among SMEs that technical standards simply do not adequately address their issues and challenges.[114] **Table 5** below lists some popular cybersecurity frameworks that can provide a baseline for the local business community as it considers which legal and regulatory approach best addresses the needs of the community. When deciding on the appropriate standards framework, advocacy groups and enterprises should weigh the following factors: 1) **whether the framework applies to the business or industry**; 2) **whether the standards required give adequate protection**; 3) **the role of the enterprise, as buyer or supplie**r; and 4) **the context of use.**[115]

Table 5. Cybersecurity Standards

Framework	Standard-setting Body	Key Components
ISO/IEC 27001	International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)	• Specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system in an organization. • Requirements are generic and intended to be applied by all organizations regardless of type, size, or nature, which makes them widely used and recommended.
Cloud Controls Matrix	Cloud Security Alliance	• Gives detailed understanding of security concepts and principles in 13 domains.
NIST CSF	National Institute of Standards and Technology	• Spans functions: Identify, Protect, Detect, Respond, and Recover. • Divides implementation into tiers, under which a company can choose how rigorous a cybersecurity framework it wants to implement.[116]
Critical Security Controls	SANS Institute	• Includes a list of 20 controls that are designed to prevent cyber-attacks and facilitate recovery. Examples include the creation of inventory and control of hardware and software assets, continuous vulnerability management, and incident response and management.[117]

Source: New Markets Lab (2018).

Institutional Frameworks Related to Cybersecurity

Given the multi-layered and highly technical nature of cybersecurity, governments need to consider a holistic institutional framework to support the legal framework. Different functions to consider include: 1) **legal and regulatory bodies to implement rules and regulations**; 2) **technical capacity to identify and respond to cyber threats**, as embodied by the National Computer Security and Incident Response Team in Rwanda, the Computer Emergency Response Team of Mauritius (CERT-MU),[118] and CERT in the EU; 3) **capacity-building to raise awareness**, provide training, and develop resources; and 4) **cooperation among inter-agency, national-subnational, and international partners**.[119]

Cybersecurity tools were mainly developed by businesses and later transformed into regulations. Participating actively in any regulatory process would benefit businesses by allowing them to share concerns with policymakers. Companies could also help design programs that address their particular cybersecurity needs through dialogue with the public sector.

Sometimes a sector-specific institutional framework could guard cybersecurity in particularly sensitive sectors. In Sri Lanka, a collaboration between the Central Bank of Sri Lanka and the Sri Lanka Computer Emergency Response Team, steered and funded entirely by the banking sector, has led to the creation of the Financial Sector Computer Security Incident Response Team (FINCSIRT). FINCSIRT receives, processes, and responds to computer security alerts and incidents affecting banks and other licensed financial institutions in the country.[120] The case study located in the Summary guide on page 30 describes how Tunisia created a task force to help strengthen cybersecurity frameworks.

Legal Deep Dive – Electronic Payments (E-Payments)

E-commerce enables the different actors along the supply chain to exchange goods and services through digital platforms. An electronic transaction or e-transaction occurs when actors make an agreement conducted over computer-mediated networks to provide goods or services. Electronic transactions of goods require the buyer to authorize and make a payment through digital means and the seller to authorize the shipment or supply of a service. When this is the case, the legal system categorizes these authorizations as e-signatures and the payment becomes an e-payment.

E-payments have become widely adopted in recent years thanks to the massive penetration of mobile phones and smartphones throughout the world. Similarly, e-signatures are fundamental not only to authorize e-payments, but also to conduct other types of electronic contracting, which is now emerging as a substitute for handwritten contracts. Regulatory approaches must balance different policy considerations including efficiency, transparency and security.

This deep dive into the legal and regulatory frameworks governing e-transactions presents some examples of the different regulatory approaches for both e-payments and e-signatures used across the world. It also addresses key considerations for both the local business community and regulators as more countries begin enacting and implementing e-payment and e-signature frameworks. This deep dive begins with an overview of the international and regional frameworks in place for e-payments. It next outlines some common regulatory approaches, specific challenges related to implementation and enforcement of laws and regulations, and examples of institutional frameworks. The E-Transactions section within the Summary Guide contains further advocacy guidance for the local business community, including a checklist for analyzing existing local electronic transaction laws and regulations.

International and Regional Frameworks for E-Payments

As domestic markets become increasingly connected at the international level through cross-border e-commerce and digital trade, a single international e-payment system or set of standards will become more pressing in order to facilitate viable, convenient, and affordable transactions. International e-payments hinge on the ability of different payment services systems to work together, which is difficult to achieve due to a lack of harmonized regulations and variations across different platforms.[121] The business community must contend with limited e-payment options, which currently include credit card companies and global services such as PayPal. More dynamic legal and regulatory frameworks will be needed if the law is to keep pace with innovation in a way that helps markets grow. That said, several multilateral and regional frameworks exist or are under negotiation related to e-payments, which provide helpful examples of ways to address regulation of e-payments. These frameworks are summarized in **Table 6**. In particular, regional frameworks provide more specific examples of regulatory approaches, which could inform business community engagement domestically and in the context of future agreements.

Table 4. International and Regional Frameworks for Cybersecurity

Frameworks	Implications for the Business Community
Multilateral	
• WTO Trade in Services Agreement (under negotiation) • World Bank's Financial Inclusion Global Initiative (non-binding)	• The WTO Trade in Services Agreement aims to further the liberalization of services and expand services market access, including financial services. Thus, e-payment systems (and e-payment providers as service suppliers) will be affected. This agreement, which is still under negotiation, could be a priority for international advocacy efforts. • The World Bank's Financial Inclusion Global Initiative brings together both governments and the private sector to improve access to finance and boost consumer trust in different forms of e-payments in three pilot countries (Mexico, Egypt, and China).

Regional	
• NAFTA (under re-negotiation) • CPTPP • Directive of the European Parliament and Council on Payment Services in the Internal Market (PSD2)	• E-payments frameworks at the regional level contain example regulatory approaches, which could inform positions taken by the business community domestically and with respect to future agreements. • E-payments are a key issue in NAFTA is re-negotiations. • The CPTPP obliges parties to avoid any unnecessary regulatory burden on electronic transactions and is progressive in the fact that it facilitates input by interested persons in the development of national electronic transaction frameworks. This provides the business community within each CPTPP member country with a more direct channel for participation in the domestic policymaking process. • The PSD2 serves as an example of a more stringent regional requirement, since businesses must have authorization to operate. PSD2 establishes controls on business organization registration requirements and security standards.

Source: New Markets Lab (2018).

Regulatory Approaches to E-Payments

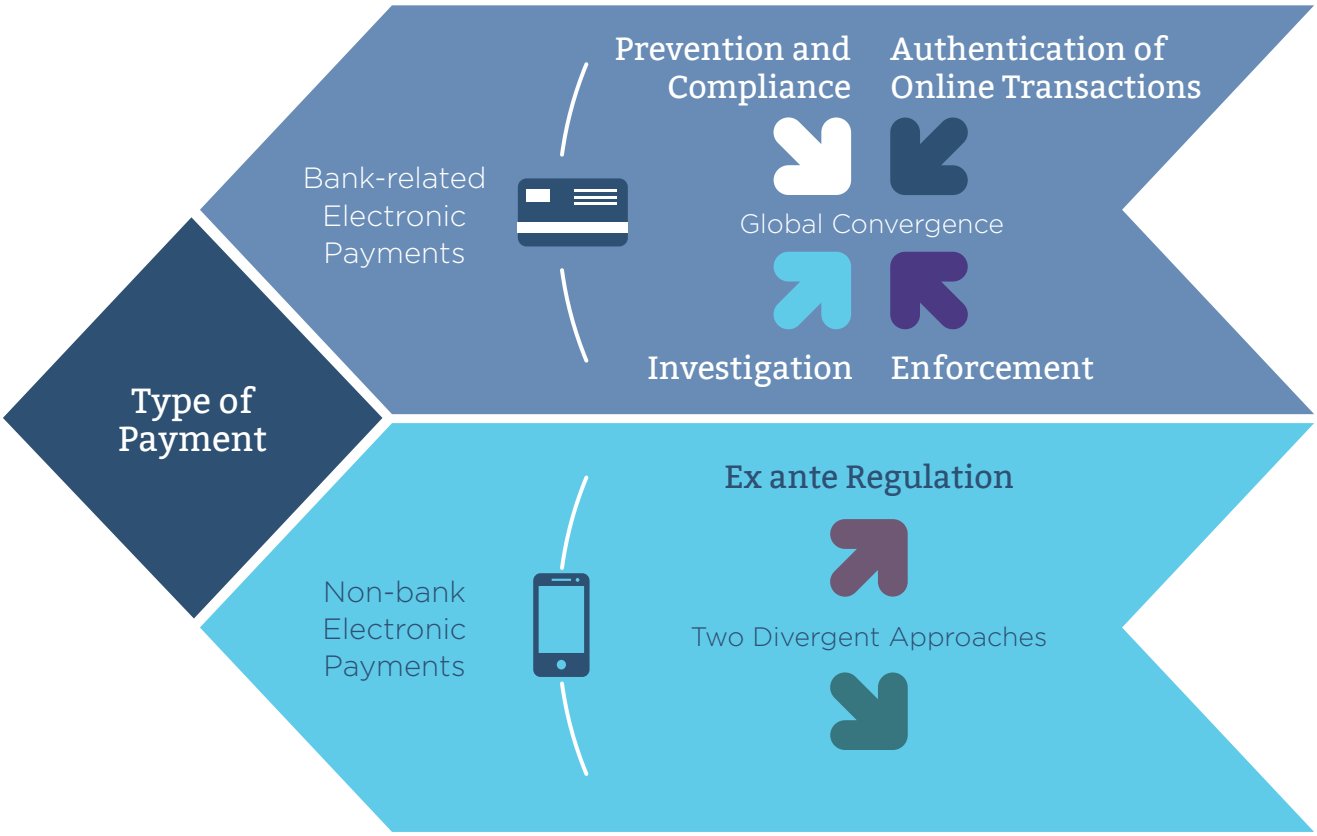
E-payment systems are regulated for much of the same reason that traditional financial services are. Governments want to foster financial inclusion, protect consumers (who will often not have as much information as the e-payment service provider), and promote a healthy environment for business and investment. Companies, of course, will want to meet growing market demand through electronic channels in a way that is both flexible and dynamic.

Regulation of e-payments tends to fit into two categories: traditional or bank-related e-payments, and non-bank e-payments. These categories are regulated differently.

Bank-related e-payments are those connected to banking systems and include debit cards, credit cards, and Automated Clearing House (ACH) accounts. Non-bank e-payment systems are those provided by non-bank intermediaries. Examples include Bitcoin, the M-Pesa and digital wallets such as PayPal and Alipay.

Overall, bank-related e-payments are heavily regulated across the globe, with most jurisdictions incorporating provisions on prevention and compliance, authentication of transactions, investigation, and enforcement. In contrast, regulatory systems for non-bank e-payments often follow one of two approaches: an ex ante approach that places regulatory controls on non-bank e-payment systems, and an ex post approach focused on enforcement, with less restrictive conditions for market entry. **Diagram 4** summarizes current regulatory approaches, and the following sections provide further detail on each of the types of e-payment systems.

Diagram 4. E-payment Regulatory Approaches



Source: New Markets Lab (2018)

Bank Related E-Payments

For many merchants and consumers, access to the banking system is the first hurdle in both electronic and traditional commerce. According to the World Bank, in 2014, 2 billion adults lacked access to the banking system or were underserviced; 55 percent of these were women.[124] Small retailers and their potential customers often face high banking fees; they might also lack the necessary paperwork to open bank accounts, or funds for indirect costs (such as travel to a bank or ATM). Other stumbling blocks include economic and labor informality, financial illiteracy, and unmet gender, religious, or cultural needs; and financial illiteracy.[125] Regulators generally aim to overcome these challenges by placing the burden on businesses that adopt bank-related e-payments to comply with legal requirements.

Regulatory approaches worldwide are beginning to converge. In most jurisdictions, key aspects include:

Prevention and Compliance: Regulators commonly work to ensure that e-payments are completed in a fair and transparent manner. As advocacy groups press for reforms or new e-payment regulations, they should determine the best course of action based on the needs of member organizations. Regulators should keep in mind that all stakeholders involved in an e-payment have a certain balance of rights and obligations. While these obligations vary from one jurisdiction to another, some of the most common prevention and compliance measures are:

- **Licensing:** Many jurisdictions, like Australia[126] and Switzerland,[127] require card issuers such as banks or financial institutions to obtain licenses to operate;
- **Due Diligence:** Businesses that are interested in providing bank-related e-payments must satisfy reporting obligations related to other policy concerns, such as anti-money laundering programs, counter-terrorism, and tax transparency,[128] including international anti-money laundering standards;[129] and
- **Consumer Protection:** To comply with consumer protection obligations, regulators often require businesses to 1) **properly disclose the cost, terms, and conditions of the transaction prior to the authorization** (as in Paraguay,[130] Mexico,[131] and the EU[132]); 2) **limit the fees they charge customers**, including credit and debit card fees;[133] and 3) **limit the financial responsibility of consumers for unauthorized charges**, **merchandise ordered but never received, goods and services not accepted by the customer, double charges and other incorrect charges in the transaction** (as in Colombia,[134] Argentina,[135] and Kenya[136] for example).

Authentication of Online Transactions: Merchants have an obligation to provide a secure environment for transactions, and different regulatory systems apply a variety of authentication mechanisms. The Payment Card Industry Data Security Standard (PCI DSS) has become a global industry standard[137] that determines authentication requirements based on company size.[138]

Investigation: Many jurisdictions have strict safeguards for customers who report suspicious or unapproved transactions.[139] In such systems, when a customer cancels a transaction or reports one as suspicious to avoid any chargeback fees, banking institutions are required to initiate an investigation of the challenged fee, and follow the legal time limits applicable in different jurisdictions.[140] If a merchant does not address a customer's complaint in a timely manner, or fails to use due diligence to confirm the cardholder's identity, the card network will charge a processing fee and a chargeback fee.[141]

Enforcement: Notably, many bank-related e-payment systems use private enforcement through industry self-regulation. For example, under the PCI DSS, noncompliance can lead to sanctions by the card network, such as fines and termination of merchant accounts.[142] Challenges related to enforcement of e-payments are covered in further detail below.

Non-Bank E-Payments

Unlike traditional bank-related or account-based e-payments, non-bank e-payments tend to be regulated differently in different countries. Regulations typically fall across a spectrum, and the local business community should determine where along this spectrum their jurisdiction falls. At one end is ex ante regulation, whereby regulators proactively determine the requirements for entering and operating in the market before the service is launched. At the other end is ex post regulation, whereby regulators choose to monitor existing payments systems rather than make additional rules on market entry and operation. The ex post style tends to encourage dynamic growth in the industry, although ex post systems can initially pose capacity challenges for some countries. Additionally, it is possible that countries with a more ex ante regulatory approach will shift to more structured systems over time.

Ex Ante Regulation: Businesses in ex ante jurisdictions must gain approval to operate through either 1) **case-by-case regulatory approval** (usually by the same institutions that oversee the banking system) or 2) **broader regulation**. India provides an example of the case-by-case approach, where the Reserve Bank of India must pre-approve any proposed novel payment systems.[143] The EU takes a broad ex ante approach through the PSD2, which regulates all e-payments, including non-bank e-payments, through newly created categories of institutions and services related to payment initiation and account information. Both approaches may benefit the local business community, but they also have some downsides. Case by case approval could preserve regulatory flexibility for new technologies, but lengthy applications and the need to familiarize regulators with new systems and technologies may be burdensome for smaller enterprises. While broad regulation may make it easier to encourage stakeholder awareness and participation, this type of approach tends to be a bit less flexible.

Ex Post Regulation: Under this approach, e-payment services are closely monitored but not necessarily subject to market entry regulations. Businesses tend to favor an ex post approach for its ease of market entry. Such an approach can also help spur innovation, because businesses need not worry that their technology will become invalid under the law.[144] Kenya's mobile money transfer system M-PESA is a good example (see case study below).

Case Study:
The Regulation of M-Pesa in Kenya

M-Pesa is a non-bank mobile payment system that only requires the use of a mobile phone and SMS and has contributed to a reduction in financial inequality in Kenya. While M-Pesa is licensed as a non-banking institution, the bank accounts are regulated by strict banking laws. This keeps M-Pesa financially stable. The Central Bank of Kenya closely monitors M-Pesa's activities but has not enacted additional regulations.

The installation and registration processes under M-Pesa are simple and free. Some 36,000 merchants accepted payments through M-Pesa since 2016. Users deposit credit either through cash deposits or an app that allows the user to link his or her bank account to their M-Pesa account. Once the money is in the M-Pesa system, the user can transfer funds to friends, family, or merchants through text message. Each transaction is priced based on a tiered structure, which allows even the poorest customer access to the network. When the cash or funds are received by M-Pesa, they are deposited in bank accounts and held in trust.

While similar models have been successful in several countries, including Paraguay, Honduras and El Salvador, mobile banking models have been less successful in places like South Africa and India. In theory, the model has broad applicability, needing just a mobile provider to create the platform for payments and money transfer. However, in practice the model seems to thrive in markets where the regulators become active stakeholders and help lead innovations. This case study illustrates that it is vital for the local business community to take a holistic approach to advocacy efforts, and work with regulators to determine which reforms would best inspire innovation and growth.

Sources: "Innovation in Electronic Payment Adoption: The Case of Small Retailers," World Bank Group and World Economic Forum, June 2016. International Finance Corporation, M-Money Channel Distribution Case – Kenya. Web; Pablo Arabéhéty García. The Replication Limits of M-Pesa in Latin America. CGAP, July 2016; Leo Mirani. Why mobile money has failed to take off in India. Quartz June 2014; Anna Leach, "17 Ways to Take Your Innovation to Scale". The Guardian. Web. July 18, 2014.

Implementation and Enforcement of Regulations Related to E-Payments

As noted above, access to banking service remains a considerable challenge for many local businesses and consumers, and bank-related e-payments may be subject to any number of regulatory requirements. Even though there is a growing presence of non-bank, alternative payment service providers, it can be difficult for both these new providers and regulators to properly implement laws in a way that keeps pace with innovation. To assist both enterprises and regulators, "regulatory sandboxes" have emerged as a solution to navigate the complex web of financial regulations while also facilitating enforcement. The term regulatory sandbox, coined in the UK, refers to a legally safe space for businesses to test new products, services, business models, and delivery mechanisms without adverse legal repercussions, all subject to monitoring by regulators.[145] This allows products to reach the market that might otherwise never have been launched or even tested.[146] Other benefits of these mechanisms include better access to finance and payment services that reach the market faster and at lower costs.[147] The UK, Australia, Singapore, Hong Kong and the Netherlands have already implemented regulatory sandboxes to promote innovation in the e-payment industry. As shown in the case study below, they provide unique opportunities for businesses to work closely alongside regulators, not only on enforcement and implementation issues, but also to highlight particularly burdensome regulations and, potentially, to participate in the lawmaking process.

Case Study:
Regulatory Sandbox for Luno in the UK

The UK's Financial Conduct Authority (FCA) was the first regulator to adopt regulatory sandboxes to promote FinTech products in the market. The initiative took effect in June 2016 and gives applicants two six-month periods per year to test their products. The main objective of the regulatory sandbox experiment was to provide firms "access to the regulatory expertise that the sandbox offers to reduce the time and cost of getting ideas to the market."

Once a firm is accepted into the sandbox it is assigned a case officer from the FCA, who helps them design the testing environment for their business model. The case officer also provides legal guidance in understanding any rule or regulation applicable to the firm's business model, including any interpretation of requirements that the firm must meet. Additionally, to facilitate the testing process, the FCA has the ability to waive or modify any unduly burdensome rule that could hinder the firm's performance in the sandbox.

A successful example of a sandbox tested company is Luno, a South African startup that developed a blockchain-enabled cross-border remittance service. Under the supervision of the FCA and in cooperation with banking partners, Luno tested the effectiveness of sending money from developed to developing markets using decentralized digital currencies. Marcus Swanepoel, CEO and co-founder of Luno stated that "We have worked closely with many different regulators around the world and our interaction with the FCA has certainly helped improve our understanding of regulatory issues affecting our business."

According to the FCA's 2017 Regulatory Sandbox Report, it is still too early to draw overreaching conclusions on the sandboxes' overall impact. Nevertheless, results from 2017 already show progress in promoting competition and inclusion in the financial sector. Seventy-five percent of the initial applicants in the first year have successfully completed testing, and 90 percent of these products continued towards a wider market launch.

Source: EY, As FinTech evolves, can financial services innovation be compliant? The emergence and impact of regulatory sandboxes- in the UK and across Asia-Pacific. Web. 2017; FCA, Regulatory sandbox lessons learned report. Web. October 2017; Paul Golden, Regulation and Innovation Thrive Together in The FCA's Sandbox, Euromoney. Web. February 22, 2017.

Institutional Frameworks Related to E-Payments

Another complex aspect of e-payments are the complicated institutional frameworks that exist around the globe. At the national level, many jurisdictions have a multi-agency structure. For example, in the US, six different agencies control oversight of depository institutions, traditional or account-based payment services.[148] Three more agencies deal with non-depositary institutions, such as non-bank e-payment services.[149] A multi-agency structure puts heightened pressure on companies to monitor and comprehend sometimes conflicting regulations and guidelines. There is less of a burden on companies when regulators coordinate to issue consistent rules, make information accessible, and alert companies of regulatory updates through a wide range of channels, such as social media accounts or mailing lists.

Jurisdictions also allocate responsibilities between national and sub-national entities differently. Some places, such as the US and Canada,[150] have delegated more responsibility at the sub-national level. For instance, non-bank payment providers must obtain a new Money Transmitter License in each state in which the provider plans to operate.[151] In contrast, the EU allocates much of the financial supervision at the Union level, with the European Central Bank and the European Banking Authority overseeing most of the financial supervisions. Similarly, India's Reserve Bank strictly supervises financial institutions operating in the territory.[152]

While some jurisdictions have established specialized new institutions focused on e-payments, this is not yet the norm. As business advocacy groups navigate existing institutional structures, they should consider the new institutional models that have arisen.

Electronic Signatures (E-Signatures)

In addition to e-payments, e-signatures are a critical aspect of transactions completed in the digital economy. Traditional handwritten signatures are an established part of contract law; however, with the rise of purely digital agreements, the concept of e-signatures poses unusual legal challenges. In its simplest form, an e-signature is a computer-based personal identity. Over the last few decades, e-signatures and associated security concerns have become increasingly complex, ranging from basic electronic copies of a person's handwritten signature to digital signatures that involve third-party certifiers.

International Frameworks for E-Signatures

Several multilateral and regional frameworks are applicable to e-signature. At the international level, most of the efforts have been led through the United Nations Commission on International Trade Law (UNCITRAL) and its Model Laws. As the core legal body of the United Nations system in international trade law, UNCITRAL has promoted harmonized and modern rules on commercial transactions through a range of initiatives, including model laws and rules with global acceptance.[153] These frameworks contain useful examples of specific provisions, which both regulators and the business community can use as useful starting points for reform or advocacy. Additional international frameworks are summarized in **Table 5** below. Some regions, such as Latin America, have already adopted the UNCITRAL Model Law on Electronic Signatures. Widespread adoption over time could help consolidate multiple frameworks, making it easier for enterprises of all sizes to operate across borders. The local business community should watch developments in this area closely and seek out areas where they can participate in the rulemaking process whenever possible.

Table 5. International and Regional Frameworks for E-Signatures

Frameworks	Implications for the Business Community
Multilateral	
• UNCITRAL Model Law on Electronic Commerce[154] • UNCITRAL Model Law on Electronic Signatures[155]	• The UNCITRAL Model Laws serve as useful starting points for discussion around specific legal provisions on e-signatures. They have been used as guides to inform domestic regulation, as in a number of Latin American countries, and could be useful tools for the local business community. • The UNCITRAL Model Law on E-commerce promotes functional equivalence between digital messages and handwritten ones, which amounts to legal recognition of electronic contracts. It also recognizes electronic signatures as a way to sign electronic documents and emphasizes equal evidentiary weight to both digital messages and handwritten documents.

	• The UNCITRAL Model Law on Electronic Signatures reflects a technology-neutral approach and non-discrimination of foreign electronic signatures (electronic signatures are treated alike, and validity of an electronic signature instead hinges on technical reliability)
Regional	
• The Latin American Integration Association (ALADI) Digital Certificate of Origin[156] • Southern Common Market (MERCOSUR)[157] • Unified Central American Customs Code (CAUCA)[158] • African Continental Free Trade Area (AfCFTA)[159]	• Regional frameworks for e-payments all contain example regulatory positions which could inform positions taken by the business community domestically and with respect to future agreements. • The Latin American Integration Association Digital Certificate of Origin aims for gradual harmonization and acceptance of forms of e-signatures. This type of transitional law might be suitable for business communities in jurisdictions with limited capacity. • MERCOSUR recognizes the validity of electronic signatures within the entire region, making it easier for the business community in this region to determine baseline standards; this could be a good practice for other regions. • Both CAUCA and AfCFTA recognize the use of electronic signatures for trade between their members, simplifying requirements for the local business community.

Regulatory Approaches to E-Signatures

While international and regional recognition of e-signatures is becoming more common, there is still a relatively fragmented approach to their regulation at the domestic level. This means enterprises engaging in international trade may have to consider multiple requirements in order to guarantee the validity of their contracts, which can be challenging for all but the largest of companies. Still, common regulatory trends exist no matter the approach used. For example, most jurisdictions recognize that the validity of contracts depends largely on the intent of the parties to be bound by an agreement, regardless of whether the contract is written, electronic, or verbal. Argentina,[160] New Zealand,[161] and Canada[162] all recognize the validity of electronic contracts through legislation or regulation. In addition to confirming that e-contracts have the same status as traditional contracts, most jurisdictions now accept electronic signatures in the course of regular business and consider them enforceable in court.

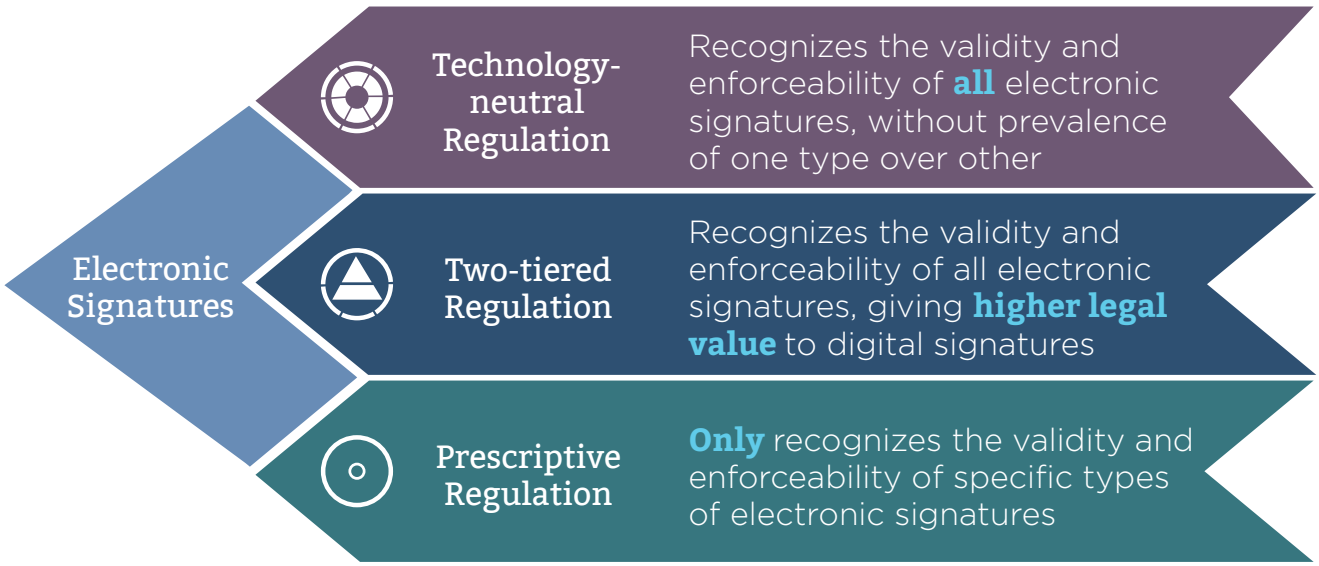
Nevertheless, many jurisdictions also establish exceptions that explicitly invalidate certain categories of e-signatures. While countries differ in their specific lists of exceptions, these commonly surround inheritance and family law issues such as divorce.[163] Others also exclude specific legal processes, such as the granting of power of attorney in India and the exclusion of notarization in Brazil.[164] In Latin American countries, even though the use of electronic signatures is widely recognized for business-related documents, the use of written signatures and notary services is still mandatory for public documents or certain types of contracts (such as real estate contracts).[165] Similarly, judges in the state of California in the US have decided that even though digital signatures are appropriate in many business settings, they do not constitute an absolute replacement for original handwritten signatures.[166]

For this reason, one of the most important questions the local business community should first ask is how its jurisdiction defines different types of e-signatures and whether these are treated differently under the rules. There are three main types of e-signatures, which vary in the level of security they provide:[167]

1. **Click-To-Sign Signatures:** These include tick boxes, e-squiggles, scanned images, and typed names;
2. **Basic E-Signatures:** The signer applies their hand-signature hand to the document electronically and the document as a whole is protected with a cryptographic digital signature owned by a service provider organization that acts as a "witness" to the signing;
3. **Digital Signatures:** These are the most advanced and secure type of signature. They use a certificate-based digital ID issued by a Certification Authority (CA) or Trust Service Provider (TSP), which uniquely links the signature to the identity of the signer. Usually, Public Key Infrastructure (PKI), a means of authentication and access control over untrusted networks,[168] is used to verify the integrity of the document.[169]

Jurisdictions tend to regulate e-signatures under one of three regulatory approaches, which will impact how different types of e-signatures are treated in terms of their validity, legality, and admissibility in court. These three approaches are illustrated in **Diagram 5** and elaborated below.

Diagram 5. E-Signature Regulatory Approaches



Source: New Markets Lab (2018)

Technology-Neutral Systems: These laws or regulations treat handwritten signatures and e-signatures equally, regardless of the underlying technology.[171] Examples of countries with technology-neutral laws or regulations include Australia,[172] New Zealand,[173] and Canada.[174] A more technology-neutral approach is the least burdensome for the local business community, encourages parties to enter into e-contracts, and promotes the diffusion of specific technologies and e-contracts.

Two-tiered Systems: While these legal systems also accept the legality and enforceability of all e-signatures, they consider certain types of e-signatures more legally valid, depending upon the security level provided by their authentication systems.[175] Examples of frameworks with two-tier systems include the EU,[176] most Latin American countries,[177] and Russia.[178]

Prescriptive Systems: This approach is the most restrictive and technology-specific, and it does not consider all e-signatures legally valid. Some prescriptive systems also impose legal sanctions when an e-signature falls outside of a specified list of legal e-signature schemes.[179] Examples of prescriptive systems include India,[180] Malaysia,[181] and South Korea. This approach could create barriers for some members of the local business community and limit new types of signatures or technologies.[182]

Implementation and Enforcement of E-Signatures

Because it often falls on judicial bodies to determine the definitions and classifications of e-signatures, the challenges that have arisen with respect to implementation and enforcement tend to be primarily in the public sector. In China, for instance, some judges are averse to recognizing e-signatures despite the law's clear recognition of them.[183] As policymakers work to enact rules that clarify the status of different types of e-signatures, business advocacy groups should work as closely as possible with the public sector to ensure their needs are met. The local business community has already been successful in working with regulators on campaigns targeting the enforcement of e-signatures, as in the case of Sri Lanka in the Summary Guide. This model could be replicated in other jurisdictions.

Institutional Frameworks Related to E-Signatures

The institutional framework surrounding e-signature also depends upon whether the law gives special value to different technologies, as well as the general regulatory framework. In technology-neutral jurisdictions, the institutional framework needed to enforce e-signatures is the same as the framework for traditional signatures: namely, courts and arbitral bodies that adjudicate contracts. On the other hand, many jurisdictions with technology-specific regulatory approaches, including most prescriptive and two-tiered systems, have created a completely independent institutional framework for the enforcement and validation of digital signatures. This framework includes both government agencies and private actors.

In such cases, some relationships and interactions are restricted by legal provisions, while others are tied completely to agreed-upon contract terms. Private actors can act as certifying bodies. These include CA or TSP, as discussed above,[184] which are common in the EU and Argentina. These regulated private actors must obtain licenses from governmental agencies, and can provide certification services if they follow technological standards. For example, the EU's Electronic Identification, Authentication and Trust Services (eIDAS) requires that TSPs be audited by a conformity assessment body, to fulfill the legal requirements.[185] In Argentina, a similar process features technological standards as well, which a company must follow to become a CA.[186] Local business communities are well-advised to take these regulated, private sector certification services as an example, as they work with regulators and existing institutions to make sure their needs are adequately addressed.

Endnotes

1. Your Dictionary, Consumer Protection Law – Legal Definition. Web.
2. OECD, Consumer Protection in E-commerce: OECD Recommendation, 2016. Web.
3. UNCTAD, Report on the Ad Hoc Expert Meeting on Consumer Protection. Web. October 23, 2012.
4. UNCITRAL, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996: with Additional Article 5 as Adopted in 1998, 1999. Web.
5. Econsumer, File a Complaint. Web.
6. European Commission: Regulation (EU) No. 2017/2394, 27 December 2017.
7. European Commission, Role of the ECC-Net. Web.
8. ASEAN, Joint Media Statement of the 48th ASEAN Economic Ministers, August 2016. Web.
9. UNCTAD, Consumer Protection in Electronic Commerce. Web. July 2017; Amy J. Schmitz, Remedy Realities in Business-to-Consumer Contracting, 58 Ariz. L. Rev. 213, 246(2016)
10. Consumer Affairs Victoria, Institutional Arrangements for Consumer Protection Agencies. Web. 2008.
11. Confianza Online, Ethical Code, Web
12. Toughnicke, Malaysian Regulation and Consumer Protection of eCommerce and Online Business. Web. May 6, 2018.
13. Korean Legislation Research Institute, Act on the Consumer Protection in Electronic Commerce, Etc. Web.
14. European Commission, Electronic Commerce Directive 2000/31/EC, Article 5.
15. for instance, in Wales and Northern Ireland, online food operators must display the food hygiene ratings given by public inspectors. BBC, Restaurants and Takeaways Must Display Hygiene Scores, LGA Says, 9 September 2017. Web.
16. Kamal Halili Hassan, E-commerce and Consumer Protection in Malaysia: Advertisement and False Description, IPEDR Vol.32 (2012)
17. For example, the Act on Specified Commercial Transactions and the Act against Unjustifiable Premiums and Misleading Representations and their guidelines. Robert Bond, E-Commerce in 25 jurisdictions worldwide. 2010. Web.
18. Advertising Standards Authority of Singapore, Guidelines on Interactive Marketing Communication and Social Media. Web. September 29, 2016.
19. Rahul Aggarwal, "A Marketer's Guide to User-Generated Content Rights and Ownership," Convince&Convert, Web. Last visited August 31, 2018. See, Draft E-Commerce Law in China, Chapter II, Section 18, 33; Competition and Markets Authority, Online Reviews and Endorsements. Web. Last updated July 27, 2017.
20. OECD, Consumer Protection in E-commerce: OECD Recommendation, 2016, Section 5. Web.
21. Latin p.12.
22. E. Luger, T. Rodden, S. Moran, Consent for All: Revealing the Hidden Complexity of Terms and Conditions, proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013. Web.
23. OECD, Consumer Protection in E-commerce: OECD Recommendation, 2016, Section 25. Web.
24. See, e.g.: European Commission, Directive 93/13/EEC, 5 April 1993, Article 3.
25. UNCTAD, Manual on Consumer Protection, 2016.
26. UNCTAD, Consumer Protection in Electronic Commerce. Web. July 2017; Amy J. Schmitz, Remedy Realities in Business-to-Consumer Contracting, 58 Ariz. L. Rev. 213, 246(2016).
27. Aspen Network of Development Entrepreneurs, East Africa Legal Guide. Web.
28. Aspen Network of Development Entrepreneurs, East Africa Legal Guide. Web.
29. Your Europe, Guarantees and Returns. Web.
30. Consumers' Rights and Interests Protection Law of the People's Republic of China (PRC), Section 25.
31. ASEAN, Consumer Protection Digests and Case Studies: A Policy Guide (Volume I). Web.
32. European Commission, Regulation (EC) 1169/2011, Article 16.
33. FTC, the US SAFE WEB Act: The First Three Years. December 2009.
34. UNCTAD, Manual on Consumer Protection. Web. 2016.
35. Consumer Affairs Victoria, Institutional arrangements for consumer protection agencies. Web. April 2008.

36. Consumer Affairs Victoria, Institutional arrangements for consumer protection agencies. Web. April 2008.

37. See CMA (UK), About Us. Web; FTC, about the FTC. Web.

38. UNCTAD, Manual on Consumer Protection. Web. 2016,

39. APEC, Data Privacy Subgroup Meeting with European Union. Web. 2017; Hunton Andrews Kurth, APEC and EU Discuss Interoperability Between Data Transfer Mechanisms. Web. August 25, 2017;

40. UNCTAD, Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR System. Web. February 2016.

41. See Mark Wu, Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System. RTA Exchange at 29, Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB). Web. November, 2017.

42. Government of Canada, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Web. March 8 2018.

43. Center for International Governance Innovation, Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. Web. April 4, 2018; Web.

44. OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Web.

45. Council of Europe, Convention for the Protection of Individuals Regarding Automatic Processing of Personal Data. Web.

46. Government of Canada, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Web. March 8 2018.

47. APEC, APEC Privacy Framework. Web. December 2015.

48. African Union, African Union Convention on Cyber-security and Personal Data. Web. June 14, 2014.

49. Economic Community of West African States, Economic Community of West African States (ECOWAS) Supplementary Act on Data Protection. Web. February 16, 2010.

50. USTR, Summary of Objectives for the NAFTA Renegotiation. July 2017

51. Government of Canada, Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Web. March 8 2018.

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

53. DLA Piper, Data Protection Laws of the World: South Korea. Web. January 16, 2017.

54. Bruno Bioni and Renator Leite Monteiro. Brazilian General Bill on the Protection of Personal Data. IAPP. Web. January 31, 2018; Bill 5276/2016 Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Web.

55. Royal College of Pathologists of Australasia, Managing Privacy Information in Laboratories. Web.

56. Regulation (EU) 2016/679 of The European Parliament and Of The Council Of 27 April 2016 on The Protection of Natural Persons with Regard to The Processing Of Personal Data And on The Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation).

57. Covington, China Issues New Personal Information Protection Standard. Web. January 25, 2018.

58. Mengyi Wang, Data Governance in the Age of Artificial Intelligence. Forthcoming.

59. Egypt Today, Parliament to make firm decision on Data Protection Draft Law. Web. January 18. 2018.

60. Center for International Governance Innovation, Data Rules in Modern Trade Agreements: Toward Reconciling an Open Internet with Privacy and Security Safeguards. Web. April 4, 2018; Albright Stonebridge Group, Data Localization. Web. September, 2015.

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

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

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

64. United Nations Conference on Trade and Development, Data protection regulations and international data flows: Implications for trade and development. 13. Web. 2016

65. Federal Trade Commission, Financial Institutions and Customer Information: Complying with the Safeguards Rule. Web.

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

67. Data Protection Commission, Registration. Web.

68. Australia's Privacy Act 1998, Section 6D.

69. DLA Piper, Data Protection Laws of the World. Web.

70. DLA Piper, Data Protection Laws of the World. Web.

71. DLA Piper, Data Protection Laws of the World. Web.

72. Linklaters, Data Protected People's Republic of China. Web.

73. National Conference of State Legislatures, Security Breach Notification Laws. Web. March 29, 2018.

74. National Conference of State Legislatures, Security Breach Notification Laws. Web. March 29, 2018

75. Regulation (EU) 2016/679 of The European Parliament and Of The Council Of 27 April 2016 on The Protection of Natural Persons with Regard to The Processing Of Personal Data And on The Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)

76. Brazilian General Bill on the Protection of Personal Data. Web.; Covington, China Issues New Personal Information Protection Standard. Web. January 25, 2018.

77. PricewaterhouseCoopers, GDPR-Data Portability. Web.

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

79. Mori Hamada & Matsumoto, Amendments to the Act on the Protection of Personal Information and Relevant Issues. Web; Mengyi Wang, Data Governance in the Age of Artificial Intelligence. Forthcoming; Nicolas & De Vega Law Offices, Data Privacy in The Philippines. Web; Begoña Cancino, Creel, García-Cuéllar, and Aiza y Enriquez, SC, Data Protection in Mexico: Overview. Web.

80. Linklaters, Data Protected People's Republic of China. Web; DLA Piper, Data Protection Laws of the World. Web.

81. "Forum Shopping" occurs when a party to a dispute recognizes that multiple courts might have jurisdiction over the claim and chooses the one that would treat his or her claim most favorably.

82. Data Protection Commission, Rights of Individuals. Web.

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

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

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

86. Mengyi Wang, Data Governance in the Age of Artificial Intelligence. Forthcoming.

87. UNCTAD, Preliminary assessment: Potential benefits for APEC economies and businesses joining the CBPR System. Web. February 2016.

88. DLA Piper, Data Protection Laws of the World. Web. Linklaters, Data Protected People's Republic of China. Web.

89. International Telecommunications Union, Definition of Cybersecurity. Web.

90. International Telecommunication Union.

91. Organization for Security and Co-operation in Europe. Cyber/ICT Security.

92. Organization of American States. Cyber Security. Web.

93. OECD, Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Web. 1 October 2015.

94. National Public Radio, Brazil's Cybercrime Free-For-All: Many Scams and Little Punishment. Web. June 15, 2015

95. Abusix, 2016 Rio Olympics: Brazil Is The 2nd Largest Cyber Crime Generator in The World. Web. August 21, 2017.

96. United Kingdom Government. The UK Cyber Security Strategy 2011-2016. Annual Report. Web. April 2016.

97. Ola Sage, Every Small Business Should Use the NIST Cybersecurity Framework. Web. 2015.

98. Cabinet Office, The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. Web. November 2011.

99. Cabinet Office, The UK Cyber Security Strategy Protecting and promoting the UK in a digital world. Web. November 2011.

100. HM Government, Small Businesses: What You Need to Know about Cyber Security, March 2015. Web.

101. Clifford Chance, New Legislation Regulating Cyber Security and the Internet in Russia. Web. September 2, 2017; Organization for Economic Cooperation and Development, Cybersecurity Policy Making at a Turning Point: Analysing a new generation of national cybersecurity strategies for the internet economy. OECD 2012. 49; Council on Foreign Relations, The Rise of Digital Protectionism: Insights from a CFR Workshop. Web. October 18, 2017; Human Rights Watch, Vietnam: Withdraw Problematic Cyber Security Law. Web. June 7 2018.

102. Clifford Chance, New Legislation Regulating Cyber Security and The Internet in Russia. Web. September 2017.

103. The Federal government defines incident as "an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system" 6 USC § 148(a)(3); the New York State Department of Financial Services regulation defines a cybersecurity event as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."

104. The Singapore Cybersecurity Bill defines "cybersecurity incident" as an act or activity on or through a computer or computer system, that jeopardized or adversely impacted, without lawful authority, the security, availability or integrity of a computer or computer system, or the availability, 10 confidentiality or integrity of information stored on, processed by, or transiting a computer or computer system.

105. Cybersecurity Act of 2015.

106. Lexology, Data Security and Cybercrime in Russia. Web. March 12, 2018.

107. Ponemon Institute. 2017 State of Cybersecurity in Small and Medium-sized Businesses (SMB). Web. September 2017.

108. Karl Flinders, UK SMEs have false sense of cyber security. Web. September 13, 2016.

109. Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.

110. This baseline amount includes a perimeter defense, such as using network firewalls and installing enterprise-grade anti-malware protection in all computers being used as part of the company. ICT personnel are also required to manage security vulnerabilities and keep systems updated with the latest software. Chieh, Lim Wei, Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.

111. Bridging the Cybersecurity Divide Between Large Enterprises and SMEs. Lee Kuan Yew School of Public Policy at the National University of Singapore. 2018. 5.

112. European Union Agency for Network and Information Security. Information Security and Privacy Standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Web. December 2015. 15.

113. European Union Agency for Network and Information Security. Information Security and Privacy Standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Web. December 2015. 19.

114. European Union Agency for Network and Information Security. Information Security and Privacy Standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Web. December 2015. 15.

115. DLA Piper, International Cybersecurity Standards: Practical Applications for Growing Corporate Value. Web. September 12, 2016.

116. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity – Version 1.1. April 16, 2018.

117. Center for Internet Security. CIS Controls. Web.

118. allAfrica, Mauritius ranks 1st on 2017 Global Cybersecurity Index in Africa. Web. June 19. 2017.

119. International Telecommunication Union. "Global Cybersecurity Index 2017." 2017. 4.

120. Sri Lanka Financial Sector Computer Security Incident Response Team. Web.

121. August Pons, Mengzhen Wang, and Lauren Sillman, Regulatory Burdens on MSMEs and E-Commerce in Lebanon, TradeLab, 2018.

122. European Parliament, Financial Services Liberalization and TiSA: implications for EU Free Trade Agreements. Web. July 2016.

123. World Bank. Financial Inclusion Global Initiative. Web.
124. World Bank, Global Findex Database 2014: Measuring Financial Inclusion around the World. Web. April 15, 2015.
125. World Bank, Payment Aspects of Financial Inclusion. Web. April 2016.
126. National Consumer Credit Protection Act 2009 (National Credit Act).
127. Financial Market Infrastructure Bank Act (FMIA) Art. 81
128. New Markets Lab/World Economic Forum, The Role of Law and Regulation in International Trade Finance: The Case of Correspondent Banking. Web. July 2017.
129. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Financial Action Task Force, 2012.
130. Ley Nº 5476 de 2015 de Paraguay.
131. Circular 29/2008 publicada en el Diario Oficial de la Federación el 11 de julio de 2008.
132. Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on Interchange Fees for Card-Based Payment Transactions, Article 12.
133. For example, the EU has capped debit card fee at 0.2 percent of the value of a transaction and credit card fee at 0.3 percent of the value of a transaction; Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 Interchange Fees for Card-Based Payment Transactions Articles 3 and 4.
134. Colombia Ley 1480 de 2011
135. Ley 25.065 de 1998 de Argentina.
136. Consumer Protection Act, No. 46 of 2012.
137. IT Governance, The 12 Requirements of the PCI DSS. Web.
138. Mastercard, What service providers need to know about PCI compliance. Web, Jacqueline Von Ogden, How Much Does PCI Compliance Cost? 9 Factors to Consider. Web. March 24, 2016.
139. These include Argentina, Columbia, the EU, Kenya, and the US, among others. See Ley 25.065 de 1998; Colombia Ley 1480 de 2011; Establécense normas que regulan diversos aspectos vinculados con el sistema de Tarjetas de Crédito, Compra y Débito. Relaciones entre el emisor y titular o usuario y entre el emisor y proveedor. Disposiciones Comunes. Web; Consumer Protection Act, No. 46 of 2012.
140. PSD2 para (71) and Chapter 6; Fair Credit Billing Act. 15 USC 160; Fair Credit Billing Act. 15 USC 160.
141. John Rampton, Accepting Credit Cards 101: What Your Business Needs to Know. Web. January 2017.
142. Payment Card Industry, Compliance Guide. Web.
143. India Payment and Settlement Systems Act of 2007, Chapter III.
144. Marianne Crowe, Mary Kepler, and Cynthia Merrit, The U.S. Regulatory Landscape for Mobile Payments: Summary Report of Meeting between Mobile Payments Industry Workgroup and Federal and State Regulators on April 24, 2012. Web. July 2012.
145. Financial Conduct Authority (FCA), Regulatory Sandbox, Web. November 2015.
146. Capgemini. Top 10 Trends in Payments 2017: What you need to know. Web. 2017.
147. FCA, Regulatory Sandbox, Web. November 2015.
148. U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Banks and Credit Unions. Web. June 2017.
149. U.S. Department of the Treasury, A Financial System that Creates Economic Opportunities: Banks and Credit Unions. Web. June 2017.
150. STI, Starting a financial institution in Canada, Web.
151. Each State has adopted laws regulating Money Transmitter Licenses, a comparative chart is available at: Thomas Brown, 50-State Survey: Money Transmitter Licensing Requirements. Web.
152. The Banking Regulation Act, 1949.
153. UNCITRAL, About UNCITRAL. Web.
154. However, these instruments are not binding, unless the signatory country decides to adopt them as such. UNCITRAL Secretariat confirms that so far 32 States have legislation based or influenced by the Model Law.
155. UNCITRAL Model Law on Electronic Signature; UNCITRAL, Guide to Enact the UNCITRAL Model Law on Electronic Signatures.
156. Argentina, Bolivia, Brasil, Chile, Cuba, Colombia, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay, and Venezuela
157. Argentina, Brazil, Uruguay and Paraguay
158. Costa Rica, Dominican Republic, El Salvador, Honduras, Guatemala and Panama have adopted the Unified Central American Customs Code.
159. Agreement signed by 44 African countries creating an African Continental Free Trade Area.

160. Section 1017 of the Civil and Commercial Code.
161. Electronic Transactions Act 2002.
162. Uniform Electronic Commerce Act (1999).
163. For instance, the Czech Republic excludes certain types of e-signatures on documents related to inheritance law. Section 1582 (2) of the Civil Code), inheritance sales (Section 1714 (3) of the Civil Code), renunciation of succession right (Section 1484 of the Civil Code)
164. DocuSign, eSignature Legality Guide, Web.
165. DocuSign, eSignature Legality Guide, Web.
166. United States Bankruptcy Court Central District of California, New Local Bankruptcy Rule 9011-1, effective December 1, 2017.
167. SigningHub. Electronic Signatures: Understanding the Different Levels and Types. Web.
168. Hongkong Post e-Cert, Concepts of PKI. Web.
169. Adobe, Adobe Sign - Digital Signature FAQs. Web.
170. Adobe, Adobe Sign - Digital Signature FAQs. Web.
171. SigningHub. Electronic Signatures: Understanding the Different Levels and Types. Web.
172. Electronic Transactions Regulations 2000.
173. Electronic Transactions Act 2002.
174. Uniform Electronic Commerce Act (1999).
175. OASIS PKI, Electronic Signature Laws and Regulations. Web.
176. The European Union's Regulation №910/2014.
177. DocuSign, eSignature Legality Guide. Web.
178. Federal Law of the Russian Federation No. 63-FZ on Electronic Signature 2011.
179. Federal Law of the Russian Federation No. 63-FZ on Electronic Signature 2011.
180. Information Technology Act 2000.
181. Digital Signature Act 1997.
182. South Korea's prescriptive approach has even resulted in enterprises maintaining outdated authentication systems. The case of South Korea and its financial transactions clearing technology is a good example of the effects a prescriptive regulatory system for e-signatures can have. Scott J. Shackelford, Scott Russell, and Jeffrey Haut, Bottoms Up: A Comparison of Voluntary Cybersecurity Frameworks. Web. 2016.
183. DocuSign, eSignature Legality Guide, Web.
184. The European Union's Regulation №910/2014.
185. Section 3 of the The European Union's Regulation №910/2014.
186. Argentina Law 25506 Firma digital.