Cross-Border Data: Managing the Risks

By:
Robert Hopen

Focus on four areas to mitigate the danger of data transfer across borders

Cross-border data transfers are not only frequent, but often crucial components of everyday business. Today's patterns of global data flow would be unrecognizable to a technologist of 20 years ago, and developments in global communication networks and business processes continue to evolve at a rapid pace.

Along with a general increase in cross-border data activity, there has been an associated increase in cross-border litigation – and, therefore, in data discovery activity. Discovery cases involving law and regulations including the Foreign Corrupt Practices Act (FCPA), International Traffic in Arms Regulations (ITAR), Commercial Bribery Crimes under the criminal laws of the People's Republic of China, and the UK Bribery Act have also risen dramatically.

These advances in data transfer technology have delivered a host of business and user benefits, ranging from the ability to take advantage of a global distribution of work and knowledge, 24-hour business operations, and convenience for users and customers.

However, this innovation has also exposed a whole new world of data vulnerability. Moreover, the unprecedented adoption of external cloud storage solutions increases the potential risks for those unaware of the provider's physical geography utilized for the storage of data. There is also the potential for violation of national and international data transfer regulations and/or privacy laws. These latter risks are becoming more common as more countries implement or update laws that regulate cross-border data transfers.

Typically, these laws either forbid cross-border transfers unless certain conditions are met or impose regulatory obligations upon the transferring companies.

Sanctions for violating the European Union's privacy regime will increase significantly with the introduction of the General Data Protection Regulation (GDPR) effective on May 25 2018 with the threat of fines up to the greater of €20,000,000 or up to 4 percent of annual global revenue. In combination with these increased sanctions, the more stringent control of EU citizen data regardless of geography stored, more frequent incidents resulting in reputational damage, and governance surrounding data storage and movement are increasingly on the radar of privacy, risk, compliance and business leaders in corporations worldwide.

Here are four key areas of focus for your company or firm to bolster data transfer across borders:

1. Awareness

Because information technology and privacy legislation around the world changes so quickly, legal and technology practitioners must be informed regarding best practices, applicable laws and regulations and security protocols to keep data safe within data centers, during transit between data centers, and in connection with a cross-border transfer. Familiarity with international data privacy and protection-related laws and regulations are also essential.

Although no generally accepted definition of the term "data privacy" exists, nor does a generally accepted framework for documenting and defining adequate "data protection"; a commonly accepted lexicon is useful.

For the purposes of this article, the following interpretations of these phrases will be used:

- Privacy – Protection of any individual's data, Personally Identifiable Information (PII) or Non Public Information (NPI).
- Data Protection – Aspect of privacy encompassing controls and safeguards that govern the processing, storage or transfer of an individual's data.

It's also important to realize that the scope of cross-border dataflow issues is often broader than anticipated. Issues can arise in numerous regulatory arenas such as financial services law, labor law, tax law, etc. However, this article focuses only on issues related to privacy and data protection.

2. Governance

Data privacy challenges often begin long before international data transfers come into play, such as at the data governance level. At present there is no standards-based model (e.g., ISO 27001) to leverage. However:

- ISO/IEC 27017 covers information security aspects of cloud computing.
- ISO/IEC 27018 covers privacy aspects of cloud computing.

ISO Standards will not address the entire scope of the privacy solution, however ISO/IEC 29101:2013 IT and Security Techniques for Privacy architecture framework, ISO/IEC 2700X series for Information technology – security techniques, and specifically ISO/IEC 27017/18 in conjunction with privacy within a cloud context start to provide guidelines and best practices when defining the nature of the systems holding PII/NPI.

The Information Governance Reference Model ("IGRM"), which can be found at http://www.edrm.net/projects/igrm, is analogous to the Open System Interconnect (OSI) Reference Model of Transmission Control Protocol/Internet Protocol (TCP/IP), as well as the Electronic Discovery Reference Model ("EDRM").

The former describes how data from an application on one computer can be transferred to an application on another computer, and the latter describes how data should move through the electronic discovery process.

The IGRM dramatically improves the ability to enable consistent interoperability between highly disparate systems and processes. The same conceptual model is required to facilitate addressing the privacy and cross-border data security challenges faced by companies today. An organization's relative information governance may also be assessed by a variety of maturity models in order to more formally benchmark progress. (See, e.g., http://www.arma.org/r2/generally-acceptedbr-recordkeeping-principles/metrics).

> A true international set of data standards has not yet been published.

3. Mitigation Strategies – Information Lifecycle

To protect data effectively when addressing cross-border data issues, you must consider the lifecycle of the relevant data. Records management models provide an excellent starting point for identifying technical and administrative security and privacy controls that apply well to cross-border data transfer challenges, acting as accountability frameworks for information management as a whole and including natural checkpoints for each step of international data transfer.

The basic components of data's lifecycle are as follows:

- Create/Capture
- Index and Classify
- Store/Manage
- Retrieve/Publish
- Process
- Archive
- Destroy

Create/Capture

How you receive or create data, whether it's captured from a website, a file transfer or a physical acquisition, will affect how it should be handled. Each point of entry requires different forms of protection. Commonly accepted secure methods for creation and capture for each type of procurement are as follows:

- Website capture: Secure Socket Layer (SSL)
- File transfer: Secure File Transfer Program (SFTP), Virtual Private Network (VPN), file encryption
- Physical: Secure media room to image and ingest the data, background checks of personnel

Index and Classify

Now that the data has been securely acquired, you must be sure to apply the appropriate rules. The first step is to identify the type of data acquired. Is it personally identifiable information (PII) or other sensitive or protected personal information? Does it contain images? Documents? What kind of documents? Carefully sifting and sorting the data into the correct "bucket types" will greatly aid compliance with international data privacy regulations.

Where programs are implemented retroactively, it is essential that consideration is given to look back across the legacy data stored in the organization. Provision of high-level characterization of the legacy content can be fed into day-forward index and classification initiatives, thus remediating any previously overlooked PII residing uncontrolled within the environment and reducing risk of unintended transfer of PII across borders.

Store/Manage

Based on classification, how do you provide adequate protection? Where will it be stored? This information will drive what protection controls are applied. If the data is PII or potential PII, then there may be a legal requirement to store the data in a disk-based encryption format and encrypt backup copies of the data. Data at rest is no less at risk of loss than data in transit. With strong characterization approaches it becomes easier to apply relevant storage regimes. Understanding if content is classified as PII determines if the data requires enhanced security, such as encryption, at the storage layer and whether the data may be stored in more cost-efficient means, such as hosted cloud, or if a local on-site facility is required.

Retrieve/Publish

The next challenge for a data transfer across borders is how to securely transfer the data across the border, and then make it available for use.

Selected examples of information privacy legislation, by region

North America

United States

- Health Insurance Portability and Accountability Act
- Fair Credit Reporting Act
- Electronic Communications Privacy Act
- International Traffic in Arms Regulations

Canada

- Personal Information Protection and Electronic Documents Act

Europe

- European Court of Human Rights, Article 8
- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data EU Data Protection Directive (Directive 95/46/EC) on the protection of personal data
- General Data Protection Regulation (GDPR), effective May 25, 2018

United Kingdom

- Data Protection Act 1998, as amended

France

- Present legislation – Law 2004-801 of 6 August 2004 modifying law 78-17 of 6 January 1978 relating to the protection of data subjects as Regards the Processing of Personal Data

Germany

- Federal Data Protection Act, as amended

Switzerland

- The Swiss Federal Data Protection Act
- The Swiss Federal Data Protection Ordinance

- Encrypt at each step of the process
  - When transferring
  - In storage
  - While displaying
- Leverage encryption key management to prevent decryption of protected data in countries to which the data is not allowed to be transferred.
- Control access to systems that can access the data and network paths that can introduce cross-border data transfers.

Process

Due care and respect for the underlying privacy law's goals must be factored into every decision to interact with data subject to protection. Thus, be sure that that data is only used for authorized purposes and in compliance with applicable laws. Application controls and metadata tagging generated during the index/classify stage are helpful during this phase.

Archive

When the data is no longer needed for production purposes, where do you store it long-term in compliance with your data retention policy and applicable legal requirements? Is the backup onsite or offsite? Do your archives or backups cross international borders? Are the backups governed by another country's privacy and data protection laws? The answers to these questions will help you to ensure that all potential risk areas are mitigated.

Destroy

At every stage, ensure protected data is rendered unusable, in accordance with applicable legislation. Ensure appropriate, documented and secure destruction of archives, files, physical copies and any other copies created during the lifecycle of the data.

Exceptions

Make sure you have processes in place for data excepted from regularly scheduled destruction cycles. Data subject to legal holds and discovery requests, as well as data exported for a case that takes it outside the ordinary retention period, is commonly excepted from data destruction for the duration of the matter at hand.

Individuals, governments and businesses all have a stake in data security.

4. Continuous Validation and Response

Even with the most robust policy, process and systems, continuous vigilance is required to validate that selected controls are effective.

- Monitor changes to the regulatory and security landscape as they rapidly advance, generating new requirements and vulnerabilities. Leverage the ISO 27001 framework for Information Security Management. This ensures a continuously improving and validated data protection and risk mitigation strategy.
- Develop a strong incident handling and remediation program to rapidly remediate identified challenges in compliance or technical security controls.
- Maintain a data map and understand how IT relates to data you store, who has access and what controls are in place.
- Characterize and regularly review stored data to ensure data storage and controls are working as expected and uncontrolled silos of data for convenience do not undermine applied policies.
- Ensure that your incident-handling program can manage a breach of data that has cross-border or inter- or multi-jurisdictional ramifications.

Conclusion

In conclusion, although much discussion has occurred around the creation of international standards for data security and privacy controls, a true international set of standards has not yet been published. Until then, meaningful protections for data – both domestic and international – will remain an issue for organizations of all kinds. Companies conducting business internationally, contracting with international vendors or hosting data with international data center providers must develop effective strategies to meet their current and future obligations related to international data transfer and data security best practices.

Overall areas of focus for increasing global data security:

- Awareness (Is your organization aware of the challenges?)
- Governance (What is your information governance model?)
- Mitigation (Are you protecting the data and meeting legal requirements at each phase of your data's lifecycle?)
- Validation and Response (Is your strategy effective? Can you adequately respond and remediate?)

Individuals, governments and businesses all have a stake in data security, whether they're directly involved or not. Staying up to date on best practices, implementing an effective, practical information governance program, identifying effective mitigation techniques, and continuous validation combined with strong incident response will enable organizations to meet the challenge of cross-border data transfers and security. Cross-border data security and privacy concerns are addressable. Follow and develop the key processes and competencies, and you'll be ready for impending regulation.

Robert Hopen

Senior Vice President & General Manager, International Markets

E: bhopen@epiqsystems.com

Robert Hopen is senior vice president and general manager for Epiq's international eDiscovery operations. His responsibilities include strategic oversight for the international business including sales, client services, operations and infrastructure support. As a member of the global eDiscovery leadership team, Hopen partners with key leaders in the international business to bring exceptional service and innovation to Epiq's global clients.