IRON MOUNTAIN®

GLOBAL INFORMATION GOVERNANCE CONSIDERATIONS FOR LAW FIRMS TASK FORCE REPORT

JULY 2015

LAW FIRM INFORMATION GOVERNANCE SYMPOSIUM JULY 2015

CONTENTS

BACKGROUND

Since 2012, the Law Firm Information Governance Symposium has served as a platform for the legal industry to collaborate on information governance (IG) best practices in the unique setting of law firms. The Symposium publications offer definitions, processes and best practices for law firm IG. In 2014, four task forces were assembled by the Symposium Steering Committee to work on specific, current law firm IG topics. This Global Information Governance Considerations for Law Firms Task Force Report outlines various factors to consider when transacting business globally.

SYMPOSIUM STEERING COMMITTEE

BRIANNE AUL, CRM
Firmwide Records Senior Manager
Reed Smith, LLP

LEIGH ISAACS, IGP, CIP
Director, Records
& Information Governance
White & Case LLP

RUDY MOLIERE
Firm Director Records and Information
Morgan, Lewis & Bockius LLP

STEVEN SHOCK
Lead Consultant / Interim Director,
Network Information Management Systems
eSentio Technologies

CHARLENE WACENSKE
Senior Manager FW Records
Morrison & Foerster LLP

TASK FORCE

KAREN ALLEN
Manager, Information Governance Technologies
Morgan, Lewis & Bockius LLP

CHRISTINA AYIOTIS ESQ., CRM
Co-Chair
Georgetown Cybersecurity Law Institute

GRACE EMANUELE
Manager, Conflicts & Records
Torys LLP

JAMES FLYNN, CRM*
Director of Records & Docket
Winston & Strawn LLP

LEIGH ISAACS, IGP, CIP
Director, Records & Information Governance
White & Case LLP

ILONA N. KOTI, MLS, MS IM, CRM,PMP, CDIA+
Principal Consultant
ARK Information Governance Consulting LLC

BRIAN B. MCCAULEY, CRM, IGP
Director of Information Governance
McDermott Will & Emery LLP

RUDY MOLIERE
Firm Director Records and Information
Morgan, Lewis & Bockius LLP

DERA NEVIN
Director of eDiscovery Services
Proskauer Rose LLP

DAVID SKWERES, IGP
Associate Director, Risk Management
Kirkland & Ellis LLP

***Task Force Leader**

SYMPOSIUM PARTICIPANTS

Iron Mountain would like to thank the following individuals for participating in the peer review sessions of the 2015 Symposium event and for sharing their perspectives and expertise during the creation of this task force report.

ANGELA AKPAPUNAM
Director of Document Lifecycle Services
WilmerHale

KAREN ALLEN
Manager, Information Governance Technologies
Morgan Lewis & Bockius LLP

DERICK ARTHUR
IG Operations Manager
Cooley LLP

BRIANNE AUL, CRM
Firmwide Records Sr. Manager
Reed Smith LLP

BRYN BOWEN, CRM
Principal
Greenheart Consulting Partners

BETH CHIAIESE, CRM, MLIS
Director, Professional Responsiblity & Compliance
Foley & Lardner LLP

SCOTT CHRISTENSEN
CIO at Large

TERRENCE COAN, CRM
Senior Director
HBR Consulting

JULIE COLGAN, IGP, CRM
Head of Information Governance Solutions
Nuix

GALINA DATSKOVSKY
CEO
Vaporstream

BRIAN DONATO
CIO
Vorys, Sater, Seymour and Pease LLP

BETH FAIRCLOTH
Director of Risk Management
Seyfarth Shaw LLP

STACEY FIORILLO
Director of Records Management
and Information Governance
eSentio Technologies

PATRICIA FITZPATRICK
Director of Information Governance & Compliance
Katten Muchin Rosenman LLP

JAMES FLYNN, CRM
Director of Records and Docket
Winston & Strawn LLP

GRANT JAMES, CRM
Senior Manager Information Governance
Troutman Sanders LLP

SHARON KECK
Director of Risk & Records Info. Management
Polsinelli, PC

CHARLES KENNEDY
Firm Director of Records and Docket
Jones Day

SAMANTHA LOFTON
Chief Risk and Information Governance Officer
Ice Miller LLP

FARON LYONS
Enterprise Account Executive
Alfresco Software

RUDY MOLIERE
Firm Director Records and Information
Morgan Lewis & Bockius LLP

DANA MOORE, IGP
Manager of Records and Information Compliance
Vedder Price PC

DERA NEVIN
Director, eDiscovery
Proskauer Rose LLP

RANDY OPPENBORN
Director, Information Governance
Foley & Lardner LLP

ALEXANDRA PROPHETE
KM Operations Manager
Cleary Gottlieb Steen & Hamilton LLP

DEB RIFENBARK, IGP, CRM
Director of Records and Compliance
Stinson Leonard Street LLP

STEVEN SHOCK
Lead Consultant / Interim Director
Network Information Management Systems
eSentio Technologies

SCOTT TAYLOR
Manager of Records, Conflicts
& New Business Intake
Smith, Gambrell & Russell LLP

CHARLENE WACENSKE
Senior Manager Firm Wide Records
Morrison & Foerster LLP

JOHAN WIDJAJA
Assistant Director Records & Information
Morgan Lewis & Bockius LLP

JOEL WUESTHOFF
Senior Director
Robert Half Legal

EXECUTIVE SUMMARY

The exponential growth of electronically stored information (ESI) creates opportunities, challenges and threats for businesses and individuals throughout the world. Many businesses mine this ESI for business intelligence and business development purposes, seeking to segment, target and contact potential customers. Criminals seek to steal that same data for unauthorized and often illegal reasons. In response, governments across the globe have adopted regulations and laws that specifically govern the use and storage of data. The lack of uniformity across these laws, as well as opportunities for conflict, amplify the management challenges faced by law firms and numerous other organizations.

Firms must address the challenges associated with data management for regulation compliance in relation not only to information regarding the operation of their business (accounting, employment, etc.), but also information received and created on behalf of clients in the course of providing legal services. While firms with office locations in more than one country are clearly impacted by these global issues, so too are firms with clients residing in, or doing business with customers in multiple countries. Further, due to the globalization of business through electronic commerce (or e-commerce), it is imperative for firms to pay particular attention to rules and regulations around data protection and incorporate a global data management strategy.

Information governance (IG) has been defined as an enterprise-wide approach to the management and protection of a law firm's client and business information assets.[1] This report will discuss how global perspectives toward fundamental issues, such as the right to privacy and data protection, shape IG requirements and the resulting implications to firms. Several key IG areas, components of the Law Firm Information Governance Framework, are highlighted within the report:

- **Cross-border collaboration**
- **Information retention**
- **Privacy and data security**
- **System configuration and data storage**
- **Information and device mobility**

Given the number of countries participating in today's global economy, a country-by-country analysis of regulations for each of these areas is beyond the scope of this report. Rather, it provides law firm managers, administrators, records and technology professionals, and others with an awareness of the IG factors that must be considered when conducting business globally.

Considering that regulations among countries are not only inconsistent, but often in conflict, there is not a single best practice to be applied in all situations. Additionally, in many instances a country's final position on these issues continues to evolve in the courts as well as other international tribunals and legislative bodies. This uncertainty and inconsistency makes one size fits all solutions impossible and requires firms to make decisions based on both their specific circumstances and tolerance for risk. More detailed information on specific countries can be found through the resources listed in the bibliography.

CROSS-BORDER COLLABORATION

Implementing and sustaining even the most basic IG program can be challenging. Cross-border collaboration introduces additional complexities on many levels as every aspect of IG becomes more complicated when firms, or their clients, operate in more than one country. Legal, compliance, cultural and other considerations create IG issues that must be considered.

LAWS, REGULATIONS AND ETHICS RULES

Just as the ABA Model Rules and individual state bar rules provide guidance on questions related to IG in the US, most other countries have similar regulations and/or ethics codes to which firms must adhere (see Table 1 below for an overview of US, Canadian and European codes).

US, CANADIAN AND EUROPEAN ETHICS CODES		
US	**CANADA**	**EU**
American Bar Association's Model Rules of Professional Conduct	Canadian Rules of Professional Conduct	The Council of Bars and Law Societies of Europe (CCBE)
Core Principles	Core Principles	Core Principles
Governs professional responsibility and ethics rules in the US	Addresses confidentiality and the need to prevent the inadvertent or unauthorized disclosure of client information	Addresses the right and duty of the lawyer to keep clients' matters confidential and to respect professional secrecy
General guidelines that have IG implications are in place, however these are vague and interpretation of these ethics rules varies from firm to firm	Lawyers must take reasonable steps to ensure that files are kept confidential and secure	Lawyer is independent and free to pursue the clients' case
	Notice must be given to clients upon receipt of their property	The firm has an obligation to avoid conflicts of interest
	Files must be clearly labeled and distinguished from the lawyer's own property	Lawyers have the right and duty of the lawyer to keep clients' matters confidential and to respect professional secrecy. In some jurisdictions the act of providing a client's address to third parties without their consent can be a violation of the client's rights
	Clients must provide consent prior to the release of any information	

TABLE 1

In the European Union (EU), The Council of Bars and Law Societies of Europe (CCBE), the Code of Conduct for European Lawyers, and the Charter of Core Principles of the European Legal Profession[2] all apply in addition to individual country requirements. These are core principles common to the entire European legal profession. Those relating specifically to information governance and client file management are:

- **The independence of the lawyer and the freedom of the lawyer to pursue the clients' case (matter mobility implications).**
- **The obligation to avoid conflicts of interests.**
- **The right and duty of the lawyer to keep clients' matters confidential and to respect professional secrecy. In some jurisdictions the act of providing a client's address to third parties without their consent can be a violation of the client's rights.**

Professional rules often differ across countries and firm administrators have a duty to inform themselves as to how these rules impact IG-related policy and decisions. Additionally, strategies for dealing with different requirements must be considered when attorneys from different jurisdictions work on the same matter. For example, due to data transfer restrictions it might be necessary for lawyers in an EU office to maintain a separate electronic file from a counterpart in the US for the same matter. Similarly, professional rules requirements may create the need for separate files for retention purposes. German laws place a much higher liability on the lawyer as an individual in malpractice cases. As a result, lawyers in Germany are much more reluctant to agree to retention disposition authorities that do not account for these concerns and do not add supplemental periods to the firm's retention schedule for the 'what if' and 'just in case' scenarios.

Matter mobility is another area impacted by local rules and regulations. While the US generally has rules that prohibit the release of client information (whether work product, client data, etc.) to third parties without client consent, other jurisdictions may not agree. Work product may be considered the property of the lawyer and failure to promptly release anything the lawyer authored may in fact be a reportable offense that can be escalated to the appropriate Law Society. In some countries, such as Ireland, the file does not belong to the client until the fees have been paid. Complicating matters, when an EU lawyer who has worked on cross-border matters leaves a firm and seeks to transfer a file, a determination must be made as to whether they are entitled to only information within their jurisdiction or in all jurisdictions in which the data resides, which may depend in part on the laws of the relevant jurisdictions. Other factors to consider during a client file transfer include:

- **Whether the firm is permitted to make and retain copies of the files post-transfer, and if so, who bears the cost of making files?**
- **Determining what files can/should be transferred and which are not considered part of the client file and thus retained. In some jurisdictions, lawyer notes do not need to be released.**
- **Whether or not the client has been charged for the creation of documents/information. As such, payment may be a determining factor as to whether the firm may withhold release.**
- **Whether it is appropriate and/or ethical to charge the client for the cost of the transfer of files.**
- **Whether the release of files can be withheld as collateral pending the receipt of monies owed/accounts payable.**

Clearly, lawyers and firm IG professionals must familiarize themselves with the appropriate ethics rules and regulations when operating outside of the US. References to ethics rules for a number of countries can be found in the professional ethics section of the bibliography.

COMPLIANCE

There are multiple governing legal codes and regulatory authorities in the international community. Compliance impacts not only information governance decisions, but can also create roles within a law firm. To illustrate further, this section will focus on compliance roles that are now required as part of rules set forth by the Solicitor Regulatory Authority (SRA) of the Law Society of England and Wales.

The SRA Handbook outlines principles and service lines that address conduct, financial and fiduciary responsibilities, disciplinary and cost recovery actions, client protection and other areas. All firms practicing under the authority of the SRA have obligatory and relevant IG dependencies.

Two roles have been created under the SRA rules that mandate firm compliance. The roles of Compliance Officers for Legal Practice (COLPs) and for Finance and Administration (COFAs) are an integral part of the SRA's objectives to achieve outcomes-focused regulation and that firms will take responsibility for managing risks in their delivery of legal services. The COLP and COFA should be champions of risk management and compliance within a firm, and will have responsibility for the firm's systems and controls. They are responsible for ensuring processes are in place to enable the firm, its managers and employees to comply with SRA Handbook requirements.

Individuals holding the role of COLP or COFA are not solely responsible for compliance with SRA Handbook requirements. Ultimately compliance is the responsibility of the firm and its leaders. However, the COLP and COFA have a key role in ensuring that suitable systems and controls are in place for recording breaches, and in reporting material breaches to the SRA. In this capacity, a regular and interactive dialogue must be maintained with the firm's practitioners supporting the IG program.

Audits, official inquiries and annual reporting on the firm's financial activities and other business practices are mandated in the SRA Handbook. As such, the firm's records will be subject to review and used to support the firm's position and potentially produced as exhibits to verify the submitted information. These records must be authenticated as valid and true. Audit logs, data protection measures, default deny settings to verify privacy and permission settings may be called upon for demonstration to verify and authenticate relevant information. The COLP and COFA roles will be dependent on a firm's IG support arm for this information verification.

CULTURAL DIFFERENCES AND DRIVERS

While drivers behind IG programs across global regions fall into the same categories such as cost savings, risk reduction, increased efficiencies and competitive advantage, the priority assigned to those drivers may vary from region to region. When implementing and/or marketing an IG program, insight into those priorities is imperative to introducing concepts and successfully moving things forward. Table 2 summarizes cultural differences in various regions and how these impact the IG strategy.

CULTURAL DIFFERENCES AND DRIVERS					
NORTH AMERICA	EUROPE	ASIA	AUSTRALIA/ NEW ZEALAND	AFRICA/MIDDLE EAST/INDIA	SOUTH AMERICA
Mitigation or avoidance of litigation	Protecting individual privacy	Quality control, process improvement and compliance	Privacy needs are similar to those in the EU	Focus on economic development	Rapid economic development in this region means a focus on competitive advantage and financial growth
Leveraging big data to gain corporate advantage	Heavy focus on business process improvements and efficiencies	Strong focus on ISO 9000 certification and Six Sigma	Professionals embrace an entrepreneurial spirit similar to those in North America	IG allows the capture of metrics, tangible results	Reaction to the Snowden disclosures indicates that privacy is a strong driver
Risk and compliance		Failure to have an established program can result in risk of noncompliance	IG drivers in organizations in this region may be risk focused yet also driven by efficiency benefits	Fiscal growth will help drive change	
Compliance with strict data handling requirements					
Organizations tend to have more evolved, sophisticated records management and IG programs in response to eDiscovery requirements					

TABLE 2

IMPLEMENTING A GLOBAL RETENTION SCHEDULE

PERFECT SCHEDULES VS. PRACTICAL IMPLEMENTATIONS

Adding a global component to a sound information retention schedule requires an exhaustive review of reliable and pertinent sources. Information governance professionals need to consider country-specific limitation of liability periods, jurisdictional ethics opinions, legal and statutory obligations, privacy and cyber security requirements, professional governing body guidelines, and client retention and disposition requirements. Careful attention must also be given to treatment of a firm's administrative business records. Countries not only have differing requirements for how long information must be retained, but some countries mandate that hard copies also be retained.

Considering all of the aforementioned topics, it may be incredibly complex and potentially impractical to put a perfect retention schedule into practice. In many cases, the numerous rules and exceptions can result in categorization requirements that are too tedious or complicated for users to follow, causing the implementation of such a schedule to fail.

Firm information governance leaders looking to establish global retention schedules need to assess the maturity of the existing records program in order to determine its current and potential capabilities. The complexity and effectiveness of a global retention schedule implementation varies greatly depending on a program's maturity. Firms that have successfully implemented a complex domestic retention schedule may have an easier time extending a similar schedule on a global basis. Other firms may choose to take a less complex, big-bucket approach with fewer categories. Table 3 lists some specific ideas on global retention schedules that a law firm should consider (and assumes a firm has a domestic retention program in place and is adding a global component).

GLOBAL IG IMPLEMENTATION: PRACTICAL CONSIDERATIONS	
Current State and Executive Support	• Determine which aspects of the retention schedule can remain as is, and which need further review and development. • Identify whether there is a responsible senior executive or steering committee in support of developing and implementing a global retention schedule, and if so, if there is representation from all countries and practice areas.
Retention Schedule Development - Identification of Information for Retention	• Identify records categories to be included and determine whether different categories have different retention periods for the same area of law. • For firm administrative records, interview administrative staff to identify the necessary records categories. • Research jurisdictional requirements for the retention of paper files. • Inventory records that exist in only paper or electronic form. Determine whether the records retention policy or retention schedule specifies which version constitutes the official record if both paper and electronic versions of the same record exist. • Query the local practice group for input and buy-in on records categories identified (e.g., correspondence, due diligence, closing documents, etc.) for corporate matters. • Create a data map, noting the repositories or official file location of all records included in the schedule. • Determine what offsite/backup storage is in place for records and if they are addressed in the retention schedule.

TABLE 3

Retention Schedule Development - Retention Period Values	• Determine the operational, legal, regulatory, fiscal and/or historical value of the records as well as retention periods by country where firm offices are located. • Determine if the firm's matter management system identifies the jurisdiction of the matter. • Consider local customs, practices, laws, regulations, contractual obligations, business needs and risk tolerance of the firm. Ten years is a safe default retention period for a client file, but the firm may want to reduce the period in order to achieve other strategic goals, such as reducing offsite storage cost or managing growth of storage hardware. • Consider which jurisdiction's retention requirements will apply when non-US lawyers work on a US matter. • Consider case law or disciplinary actions taken in the country regarding records retention, particularly relating to destruction of records and cases where the courts have scrutinized the retention policies/retention schedules of firms. • If litigation is common in the country, research whether law firm records about legal representation have been called into question during discovery disputes, motions for sanctions, etc. • Countries with a history of political instability and/or natural disasters may necessitate additional controls such as backup or paper duplicates to protect records until the retention period is met. • Determine the firm's obligation to retain records of non-US lawyers in accordance with local law society rules, laws and/or regulations. • The firm may need to retain records relating to non-US lawyers longer than other matter records, or alternatively, increase retention period on all records relating to the matters that have non-US billers.
Retention Schedule Implementation	• Consider local lawyer resources available to review and approve records when they become eligible for retention review (i.e., when the retention period has been met). • Consider the native language of the records. This may impact who conducts the retention review. • Identify whether translation is necessary if English is not the official business language of the firm in all jurisdictions covered by the retention schedule. Consider the users responsible for referencing and executing the retention schedule. These are not always the lawyers. Even if English is the business language, translating into the local language (or dual language schedule) may help increase awareness and compliance, depending on the English proficiency of the local lawyers and staff.

TABLE 3 CONTINUED

Implementation of the Records Retention Schedule

- Draft a master retention schedule that includes office/country/jurisdiction specific requirement. Example:

	UNITED STATES	UNITED KINGDOM	GERMANY	HONG KONG	CHINA	CITATIONS	NOTES
Client Bills							
Client Bill	7 years	7 years	10 years	7 years	25 years	Income Tax, ABA	For certain offices, scanned copies stored in Legal database.

- Forward the proposed retention schedule for review and approval by those responsible for Risk Management, Privacy, Security and the Office of the General Counsel.
- Consider leveraging the existing home schedule with carve-outs for exceptions.
- Understand and consider the pros and cons of carve outs vs. applying the longest retention period to all records.
- Establish checks and balances to ensure that the master retention schedule will be applied in a consistent, repeatable manner regardless of office/country/jurisdiction.
- Consider committee oversight with representation from each practice area.
- Common practice is to appoint a records coordinator in each office/country to liaise with the central Records Management Department and Governing Committee.

Retention Schedule Audit, Compliance and Governance

- Require ongoing maintenance of records retention review and destruction protocol.
- Once issued, determine what the process is for making changes to the retention schedule.
- Designate a responsible person to continuously monitor local requirements and proposing revisions, additions (i.e., new retention periods for new records categories), removing categories that are no longer used or consolidating existing categories to better reflect how law is practiced.
- Consider using a vendor or service that specializes in identification of country-specific requirements to provide periodic updates.
- If firm partners are responsible for reviewing the records eligible for review per the retention schedule and approving destruction, decide whether they can delegate records retention review decision-making authority to other lawyers or paralegals.
- At a minimum, firms should be able to prove that:
  1. The schedule was distributed to all lawyers and support personnel.
  2. Training on the use of the schedule was administered.
  3. Audits were conducted to ensure compliance with the schedule.
  4. Senior management/partners were actively involved in the creation and implementation of the schedule.

TABLE 3 CONTINUED

PRIVACY AND DATA SECURITY CONCERNS

The proliferation of electronic information, particularly personally identifiable information (PII), has elevated concern over protecting individuals' right to privacy. High profile hacks of retailers and other organizations, including a major healthcare provider which exposed massive amounts of PII, serve to justify this concern. Conversely, recent acts of terrorism in the United States, Canada, Australia, France and Denmark are driving increased calls for more transparency and sharing of information in an effort to combat terrorism. Canada's Prime Minister, Stephen Harper, has introduced new anti-terror legislation giving agencies more authority to share private information. In light of

the Parisian violence in January 2015, the EU Council President is urging the European Parliament (EP) to consider sharing airline passenger data, something the EP has been reluctant to do as it would infringe on EU citizens' privacy.

Regardless of the outcomes in these two examples, the US approach to PII and right to privacy is quite different than that of the EU, Asia and other regions/countries. These differences must be taken into account by law firm IG professionals when considering data systems, storage and information transfer.

DIFFERING PHILOSOPHIES

Countries around the world have differing philosophies when it comes to individual privacy and its protection. As mentioned above, some of these differences can be attributed to a country's experience, in particular, their historical past including culture, politics and government (see sidebar).

There are three common approaches to privacy regulation:

- **Comprehensive: laws exist to cover all collection, use and dissemination of personal information in the public and private sectors (e.g., EU, Canada).**
- **Sectoral: laws exist, but only to cover specific areas where the legislative body has found a particular need (e.g., United States, Japan).**
- **Self-Regulatory and Co-Regulatory: emphasizes industry development of enforceable code or standards for privacy and data protection against the backdrop of legal requirements by the government and/or relies on stakeholders to ensure privacy protection (Australia, New Zealand).**

PRIVACY REGULATIONS

Since 1970, over 70 countries have enacted data protection and privacy laws regulating international data transfer. Appendix B contains a list of privacy laws, requirements and guidelines from across the globe. In addition, the Data Protection Laws of the World handbook published by DLA Piper LLP is an excellent source for global privacy and other data laws.[3]

STRATEGIES TO MEET PRIVACY AND DATA SECURITY REQUIREMENTS

To successfully manage issues related to global privacy and data security, the IG professional must have an awareness of the differing philosophies that exist between countries/regions, knowledge and understanding of

Privacy regulations in Germany, which are very stringent, have been influenced by the exploitation of personally identifiable information by the Nazi party prior to and during World War II. Census data was used to help identify those who belonged to disfavored groups. Jewish and Slavic people, Communists, Roma, homosexuals, and others were first discovered, singled out, and then persecuted.

the relevant acts and laws, and the ability to develop practical and enforceable processes and procedures within their firms to ensure compliance. Until recently, attempts to account for data privacy requirements have focused on configuring existing systems to meet privacy requirements. As the consequences of non-compliance continue to grow, these requirements are being factored into system design and acquisition as native functionality.

As part of this process, a data-centric rather than a technology-driven approach can be more effective. Before purchasing new technology, whether a new server or software application, firms should first determine their business data requirements and then determine how relevant privacy and security requirements apply to this data. Factors to consider include:

- **The location of offices for regulatory and legal compliance issues.**
- **The type of law practiced and any unique requirements (i.e., wills and estates).**
- **The type of clients (e.g., health sector, nuclear energy sector) and confidentiality concerns regarding operations, public company, private company, foreign client with local matter/transaction, individual, cross-border and multi-jurisdictional.**
- **The type of administrative information collected and storage locations, both internal and external if outsourced.**
- **The type of information systems in use, including client/matter intake, email management, document management system (DMS), enterprise content management system (ECM), human resources application, etc., and the integrations between them.**

Once a firm's privacy and data security requirements have been identified, an IG program can be developed to incorporate processes and procedures to meet those requirements.

Two sets of industry principles that can help in the development of a firm's IG program are the Generally Accepted Privacy Principles (GAPP) and the Generally Accepted Recordkeeping Principles[4] (The Principles). While GAPP provides guidance in creating policies and practices specifically around privacy and security, The Principles provide guidance about incorporating those policies and practices into the firm's overall IG program.

PRIVACY BY DESIGN

A systems design approach gaining momentum in recent years is Privacy by Design (PbD). PbD, developed by the former Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian, is being advocated as a proactive method for safeguarding privacy. The incorporation of PbD is explicitly listed in the EU's proposed changes under the EU Data Protection Directive (see sidebar).

Using the seven principles[5] identified as foundational to the framework of PbD, controls are built into information systems as well as operational processes to ensure personal information is stored safely and violations are prevented. In the January 2013 publication *Privacy and Security by Design: A Convergence of Paradigms*, both PbD and security by design are discussed.[6] Within Privacy and Security by Design, information systems architecture takes into account; 1) desired goals that are to be achieved through the systems; 2) the environment in which the systems will be built and used; and 3) the technical capabilities needed to construct and operate the systems and their component sub-systems. The authors suggest that bringing together privacy and security by design creates a synergistic effect that will result in information systems that are more robust, with safeguards embedded by default, as well as creating a culture of privacy across the enterprise. PbD will continue to gain momentum as privacy and data security requirements within firms continue to increase in importance and impact firm-wide information systems.

EU Proposed Changes

- **Regulation - directly applicable to all EU member states**
- **Rules extend to all foreign companies processing data of EU residents**
- **Significant penalties - up to 2% of annual worldwide turnover (revenues)**
- **Appointment of Data Protection Officer**
- **Notification of data breaches**
- **Incorporate privacy by design**
- **Right to be forgotten/erasure**
- **Data portability**

DATA SYSTEMS, STORAGE AND TRANSFER CONSIDERATIONS

In addition to system design, firms must consider data storage and transfer implications of the data protection and privacy regulations of countries in which they generate data. Regulations governing data security typically focus on the protection of both information systems (networks, software, and databases) and the data those systems create, process, communicate, receive or share. The vast majority of countries around the world define data in a similar and expansive way; any corporate compilation of data or information can be included in the concept, regardless of format (electronic or not). Most global regulations are concerned with the means of controlling access to data and assume that unauthorized access is an infringement.

In the majority of countries, there is a defined scope of what the legislation regards as protected data. Though these definitions, regulations and the associated penalties for non-compliance vary widely, most fit into the principles as defined by the EU Data Protection Directive (EU Directive 95/46/EC). In some cases, EU data protection rules are

supplanted by the individual member country's regulations and perhaps even further by regions within a country. In the US where much of the transfer from the EU occurs, the wide range of laws covering various industry sectors does not equate to an overarching law about data privacy and security deemed sufficient by the EU to provide requisite data protection.

DEFINITIONS AND USE OF UNPROTECTED DATA

The types of data transferred across borders have also changed over time. There is now much more information containing protected personal data being transferred, as well as more sharing of personal data between governments; often for law enforcement purposes such as airline passenger registries. Complying with all the global data privacy and security protection requirements has considerable economic costs and implications. Strategies that include contractual clauses and/or internal binding corporate rules and policies are increasingly used to aid compliance.

Data protection regulations have to balance competing priorities. The regulations are designed to ensure that everyone has an appropriate degree of control over the collection and use of his/her personal data. However there is still a need to promote and support the flow of data for corporate purposes. EU Directive 95/46/EC has since been updated to reflect developments in trade practices in general, and IT in particular, to provide an equal protection of personal data regardless of the technologies used. Established principles are:

- **Openness:** the data subject must be informed about the existence of automatic processed personal data files and the identity of the data controller.
- **Minimization:** the amount of data gathered should be limited to what is necessary to achieve the purpose of gathering the data.
- **Individual Access:** the data subject should be informed of and given access to the data on him/her kept by the data controller within a reasonable time and in a reasonable manner.
- **Collection Limitation:** the gathering of personal data has to be fair and legal. The collection of specific sensitive data must be prohibited (protected classes: race, political affiliation, health, etc.).
- **Purpose Specific:** personal data can only be collected and processed if it is necessary for a specific lawful purpose and based on legitimate grounds.
- **Use Limitation:** the data can only be used according to the purpose for which it was specifically collected. Any other use without the consent of the data subject is a violation.
- **Individual Participation:** any subject has the right to check data relating to him/her, to correct or have it removed from files if necessary.
- **Information Management:** data has to be adequate, correct, complete, current, and be secured against destruction, disclosure and alteration by unauthorized people.
- **Accountability:** the custodian of the data is responsible for ensuring that all principles are adhered to.

In the EU, some exceptions to these rules are provided; for instance, when the controller of the data can guarantee that the recipient will comply with the data protection rules.

DATA STORAGE AND TRANSFER CONSTRAINTS

Most countries specify that personal data may only be transferred to countries outside their borders if that country provides an adequate level of protection - though what is considered adequate varies widely. This can be beneficial in some data exchanges as the requirement is for adequacy, not equivalency, making it possible to exchange data under different methods of data protection.

Complicating the problem of international transfer of data is the comprehensiveness, strictness and enforcement of regulations that differ significantly between countries. However in recent years, leading international privacy groups such as the Asia Pacific Economic Cooperation (APEC), the International Conference of Data Protection and Privacy Commissioners, the EU Article 29 Working Party, and the Organization for Economic Co-operation and Development (OECD), have begun to address the need for cross-border cooperation in the area of data-sharing regulation enforcement. The OECD adopted recommendations that encouraged member countries to "*foster the establishment of an informal network of Privacy Enforcement Authorities and other appropriate stakeholders to discuss the practical aspects of privacy law enforcement co-operation, share best practices in addressing cross-border challenges, work to develop shared enforcement priorities, and support joint enforcement initiatives and awareness raising campaigns.*" [7] The OECD also recommended that privacy enforcement authorities *"should co-operate with each other, consistent with the provisions of this Recommendation and national law, to address cross-border aspects arising out of the enforcement of Laws Protecting Privacy."*

Great examples of this cross-border cooperation are the processes approved by the EU for transfer of privacy data, such as law firm human resources information, to the US. The US is not on the EU's list of countries deemed to have adequate data protection laws, however there are three approved approaches available to firms: join the US-EU Safe Harbor program, create and adhere to binding corporate rules (BCR) in accordance with EU requirements, or submit to one of three standard contractual clauses (model contracts) created and approved by the EU.[8] Safe Harbor is essentially a self-certification process wherein an organization must annually certify compliance with EU data protection standards. BCRs are created by the organization according to guidelines published by the EU and must be approved by the Data Protection Authority of the member state from which the data transfer will occur. Model contracts are pre-approved by the EU. Firms choose the most appropriate of these options according to their specific circumstances.

Many countries (e.g., the United States, the United Kingdom, and Australia) have export control laws that prohibit anyone but their country's citizens from accessing certain protected information no matter where the information is physically located. It is important that such data protection and handling requirements are built into systems and processes. For example in the United States, defense contractors and their global firms should consider who will have access to information regulated by International Traffic in Arms Regulations (ITAR). A brief summary appears in Table 4.

REGION EXPORT CONTROL LAWS				
EUROPE	**RUSSIA**	**AFRICA**	**SOUTH AND CENTRAL AMERICA**	**MIDDLE EAST**
Most restrictive with respect to personal data	On December 17, 2014, the State Duma expedited the Data Localization Law (requiring the local storage in Russia of the personal data of Russian citizens) effective date from September 1, 2016 to September 1, 2015[9]	Majority of African nations have no data export regulations, and there are no safe listed countries	Most countries have little or no data export regulations	While the majority of the countries have few or no data export regulations, some countries (Israel, UAE) have restrictions similar to those of the EU
Collective countries follow common law under Directive 95/46/EC and its subsequent updates			Regulations that do exist are vague, mostly stating that data can be exported to other locales with an adequate level of protection but without definition	
Countries also follow their own law, which sometimes supersedes the EU Directive				

TABLE 4

EDISCOVERY CONSIDERATIONS

Many regulations follow the principle of territoriality, meaning that data collection and production rules do not have extra-territorial effect outside the country. For example, if a company has a presence in Germany and an affiliate in France, the company can freely send personal data to the French affiliate. However, if a German company wants to

send the same data to its parent company in the US, it must comply with all German and EU rules for international data transfer to third countries without adequate data protection rules.

In addition, the concept of discovery as we know it in the US does not necessarily have an international equivalent, except perhaps in the Commonwealth countries (e.g., e-disclosure in the United Kingdom). In the US, a firm can be compelled by the court to produce information in discovery. Other countries do not necessarily recognize the same concepts and may apply their international data transfer rules and refuse to turn over the requested data citing local regulations.

CLOUD CONSIDERATIONS

Concerns with data stored in the cloud add complications for both global and purely domestic organizations since data can end up being stored in countries where there are either limited or highly restrictive governmental regulations.

When deciding to store data with a cloud provider, firms must determine who controls the data, which laws are applicable, whether the data is encrypted and if so, who has the capability to decrypt and/or produce the data, and whether the data will be crossing borders. It is essential to determine where the data is stored to determine if it can be easily transferred out of the country holding the data; if it is on a server in a country with export restrictions, the data may not be retrievable. Also, firms should consider whether local laws might compel production of data under care and control concepts even if data ends up in a country with conflicting regulations.

Many cloud provider service contracts limit the liability of the hosting provider, similar to limits of liability for a software license. As it relates to international data transfer, any agreement with a cloud provider should include language in the cloud provider's contract that, at a minimum, 1) establishes ownership of the data; 2) prohibits or limits subcontracting by the provider; 3) specifies locations where data can be stored; 4) establishes a methodology for implementing legal holds; 5) establishes access rights to the data; and 6) whether the vendor is permitted to produce firm data without getting permission from the firm and whether notice is required. These provisions will limit the number of service providers, minimize cross-border transfers and should reduce or eliminate issues with accessing the data for discovery.

CONSIDERATIONS FOR TECHNOLOGY SYSTEMS/DECISIONS

For a global firm considering where data can or should be stored, the following questions should be addressed for any country in which the data originates, or may ultimately reside:

- **What is the applicable legislation in the country where the data will be stored? Is there a government agency that must approve data transfers? If so, what does that approval process entail?**
- **What does the country consider to be PII and does it further distinguish sensitive PII?**
- **How are those protections enforced?**
- **Does the country have any restrictions on transfer of data outside their boundary?**
- **Are there specific criteria that must be met (e.g., explicit consent, public interest)?**

INFORMATION AND DEVICE MOBILITY

In the mobile era, lawyers have to weigh the benefits of maintaining constant access to client information against the risk of that information being compromised. As with personal property security and safety in general, traveling with any electronic device increases risk of loss and the complexity associated with the consequences of such loss. Lawyers and firm administrative staff crossing borders to visit firm offices or clients must take extra precautions and beware of the following factors:

- **Countries with higher crime rates in general have shown a correlation to increased data theft.**
- **Many countries have no legal restrictions against technical surveillance, increasing the vulnerability of transmitting information in public places such as hotels, airports and cafes.**
- **Most countries, the US among them pursuant to the PATRIOT Act, permit customs agents to search, detain and potentially copy data from laptops and cell phones of travelers deemed suspicious as they pass through customs.**
- **Some countries (including Russia, China and Saudi Arabia) have laws prohibiting the import of devices containing encryption software without special exemptions obtained in advance.** [10]

Given these heightened risks, firms should develop a protocol around international travel that includes the following components:

- **Notification of appropriate firm administrators when a lawyer or staff member is scheduled to travel internationally on firm business. To the extent a firm uses a centralized travel resource, they should be aware of the need to notify administrators upon booking international travel. Where the responsibility for travel arrangements is dispersed to lawyers and/or their assistants, they should know of the requirement to notify firm administration. Doing so allows the traveler to receive the appropriate security information for data protection prior to the trip, and for IT to provide any special equipment and instructions.**
- **Education of lawyers and staff regarding the information risks associated with international travel. For those traveling internationally on firm business for the first time, education is an important step. Simply reminding those who are traveling that they could be subject to very different laws and potentially corrupt behaviors on their travels can be valuable.**
- **Creation of country-specific requirements which include which type of devices employees may carry and whether the country has regulations around devices with encryption software entering the country (at least for high-risk countries and those countries frequently visited by firm employees).**
- **Regular monitoring and/or consultation of government travel alert sites such as the US Department of State.**[11] **Although travel alerts are frequently issued and usually do not involve warnings relative to the technical aspects of information theft, increased incidents of property theft or similar threats can have implications and should be monitored for employees' personal safety.**

Other recommendations for the protection of sensitive information include:

- **Unless absolutely necessary, do not carry or transmit sensitive data. Many organizations, particularly those involved in technology and research and development, will not allow employees to bring any device other than a loaner laptop or mobile phone, stripped of all information except that which is essential for the purpose of the trip.**
- **Consider use of pre-paid burner cell phones which can be discarded after the trip.**
- **Never leave any device containing sensitive information unattended (for example in a hotel room while at dinner).**
- **Clear browser of history, cache and cookies after each use.**

Occasionally lawyers are seconded to clients that may have an international presence, yet still require access to firm systems. Strategies to address security concerns in such instances can include: 1) require that the client provide a computer/portable device to the lawyer; 2) provide the lawyer with a firm laptop that has been cleaned and ensure that access to local storage (such as desktop, personal drive, etc.) is disabled; 3) require the lawyer only access firm data via a secure method such as Citrix® and/or, 4) understand that particular access methods may leave cached data behind, such as a virtual private network (VPN), therefore those methods should also be disabled.

CONCLUSION AND SUMMARY CHARTS

Regulatory complexity and risk of data loss and theft increase significantly when firms are resident, or practicing in multiple countries. The information explosion and resulting attempts by governments to regulate use of data has added many challenges to the already complex task of managing global firms. Failure to comply with regulations and properly safeguard data across borders can result in significant financial repercussions and damage to reputation. From an IG perspective, the biggest challenge confronting firms with a global practice is the multitude of additional and differing rules and regulations and their impact on firm operations. Firms should be aware of these issues and continually monitor information sources as rules and regulations frequently change.

Table 5 summarizes regional positions with respect to some of the major issues as of the date of this report. As rules and regulations continue to evolve, readers are encouraged to consult additional information sources to verify accuracy.

GLOBAL DATA REGULATIONS				
US	**CANADA**	**GERMANY**	**UK**	**AUSTRALIA**
The PATRIOT Act was passed to address terrorism financing by tightening CFT/AML processes, and is one example of how laws have affected the way firms do business	In Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA) outlines rules on how private sector organizations collect, use or disclose personal information in the course of commercial activities, unless an equivalent provincial legislation on the same topic applies	Germany's strict protection of individual privacy does not recognize Safe Harbor regulations in the same way as other EU states	The Data Protection Act includes 8 guiding principles	Australia's Privacy Act contains 13 guiding principles referred to as APPs which apply to the handling of personal information by most government agencies as well as private sector organizations
Other laws at both federal and state levels governing data privacy and impacting firms include HIPPA, GLB, ECPA, FCRA, FDCPA, NY Code - Article 6-A Personal Privacy Protection Law and California Shine the Light Law (S.B. 27)		Safe Harbor requirements include guidelines to be met by all parties involved	The UK has established the Information Commissioner's Office (ICO) to uphold and monitor compliance with the Data Protection Act	
		The Bundesdaten-schutzgesetz (BDSG), a Federal Data Protection Act (FfDF) first introduced in 1977, covers the data processing of all federal agencies including the federal government and private sector organizations	The ICO has the authority to impose fines up to £500,000 for serious data breaches	
			The proposed changes to the Directive, that dates back to 1995, includes notification of data breaches, right to be forgotten, data portability and the incorporation of privacy by design	

TABLE 5

APPENDIX A: GLOSSARY

TERM	DEFINITION
ABA Model Rules of Professional Conduct	Professional conduct rules created by the American Bar Association (ABA) that prescribe baseline standards of legal ethics and professional responsibility for lawyers in the United States. Additional information: http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html
Article 29 Working Party	Composed of representatives of the national protection authorities, the European Data Protection Supervisor and the European Commission. The main goals are to provide expert advice at the national level to the European Commission on data protection matters; promote the uniform application of Directive 95/46 (DPD) in all Member States of the EU, as well as in Norway, Lichtenstein and Iceland; and advise the Commission on any European Community law that affects the right to the protection of personal data. Additional information: https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29
Asia-Pacific Economic Cooperation (APEC)	A regional economic forum established in 1989 to leverage the growing interdependence of the Asia-Pacific region. APEC's 21 members aim to create greater prosperity for the people of the region by promoting balanced, inclusive, sustainable, innovative and secure growth by accelerating regional economic integration. Additional information: http://www.apec.org/About-Us/About-APEC.aspx
California S.B. 27, Shine the Light Law (a/k/a Sunshine Laws)	A privacy bill passed by California in 2003 that empowers individuals to learn about how businesses sell their personal information. Under the law, companies that do business with California residents have to either allow customers to opt out of information sharing, or make a detailed disclosure of how personal information was shared for direct marketing purposes. Companies with fewer than 20 employees and federal financial institutions are exempt from the law's requirements. Additional information: https://epic.org/privacy/profiling/sb27.html
Canada Personal Information Protection and Electronic Documents Act (PIPEDA)	Canadian legislation that sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. PIPEDA also applies to federal work, undertakings and businesses in respect to employee personal information. It gives individuals the right to access and request correction of the personal information these organizations may have collected about them. Additional information: https://www.priv.gc.ca/leg_c/leg_c_p_e.asp
Canadian Rules of Professional Conduct	Conduct rules imposed by the Federation of Law Societies in Canada that expects members of the legal profession to conduct themselves ethically in accordance with high standards of professionalism. Additional information: http://www.lsuc.on.ca/lawyer-conduct-rules/
CAN-SPAM Act	Law signed into effect in 2003 that sets the rules for commercial email, establishes requirements for commercial messages, gives recipient the right to stop receiving emails, and spells out tough penalties for violations. Additional information: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Charter of Core Principles of the European Legal Profession	Foundational text adopted by the Council of Bars and Law Societies of Europe (CCBE). Although not conceived as a code of conduct, it is aimed at applying to all of Europe. It contains a list of ten core principles common to the national and international rules of regulating the legal profession. Additional information: http://www.ccbe.eu/index.php?id=32&L=0
Children's Online Privacy Protection Rule (COPPA)	A Federal Trade Commission rule that imposes certain requirements on operators of websites or online services directed to children under 13 years of age, and on operators of other websites or online services that have actual knowledge that they are collecting personal information online from a child under 13 years of age. Additional information: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
Code of Conduct for European Lawyers	A legal ethics code for lawyers in the European community whose goal is to mitigate the difficulties that could result if a lawyer is subject to conflicting ethics rules. Also known as the CCBE Code. Additional information: http://www.personal.psu.edu/faculty/l/s/lst3/ccbe1withappendix.pdf
Code of Federal Regulations (CFR)	A codification of rules, including those relating to recordkeeping, published in the Federal Register by the executive and other branches of the US federal government. ARMA Glossary 2012
Council of Bars and Law Societies of Europe (CCBE)	The Council of Bars and Law Societies of Europe (CCBE) is an association gathering together bar associations of 32 countries in Europe (those of the European Union, of the European Economic Area and of Switzerland) and an additional eleven associate and observer members. The CCBE represents approximately one million European lawyers before EU institutions mainly, but also before other international organizations. The CCBE is an international non-profit organization (AISBL) under Belgian law and has its seat in Brussels. Additional information: https://en.wikipedia.org/wiki/Council_of_Bars_and_Law_Societies_of_Europe
Cross-border Collaboration	Working or engaging in business or the representation of matters between organizations in different countries. This can refer to matter management in firms that have global offices, the representation of clients/organizations with a global presence or the combination of both.
Data Localization Laws	Local jurisdictional laws that involve forcing countries to store data on their citizens within those countries' borders. Additional information: http://www.lawfareblog.com/jonah-force-hill-growth-data-localization-post-snowden-lawfare-research-paper-series
Dodd-Frank Wall Street Reform and Consumer Protection Act	U.S. Public Law 111-203, enacted in 2010 to promote the financial stability of the United States by improving accountability and transparency in the financial system. ARMA Glossary 2012
Electronic Communication Privacy Act (ECPA)	Enacted by the United States Congress in 1986. Extends government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer, added new provisions prohibiting access to stored electronic communications and added so-called pen trap provisions that permit the tracing of telephone communications. Additional information: https://en.wikipedia.org/wiki/Electronic_Communications_Privacy_Act

European Commission (EC)	The executive body of the European Union responsible for proposing legislation, implementing decisions, upholding the EU treaties and managing the day-to-day business of the EU. Commissioners swear on an oath at the European Court of Justice, pledging to respect the treaties and to be completely independent in carrying out their duties during their mandate. Additional information: https://en.wikipedia.org/wiki/European_Commission
European Convention on Human Rights	The European Court of Human Rights oversees the implementation of the Convention in the 47 Council of Europe member states. Individuals can bring complaints of human rights violations to the Strasbourg Court once all possibilities of appeal have been exhausted in the member state concerned. This is the first Council of Europe's convention and the cornerstone of all its activities. Additional information: http://www.coe.int/en/web/human-rights-convention
European Directive (EU Directive)	A legal act of the European Union which requires member states to achieve a particular result without dictating the means of achieving that result. It can be distinguished from regulations which are self-executing and do not require any implementing measures. Directives normally leave member states with a certain amount of leeway as to the exact rules to be adopted. Directives can be adopted by means of a variety of legislative procedures depending upon their subject matter. Additional information: https://en.wikipedia.org/wiki/Directive_%28European_Union%29
European Parliament	Formerly European Parliamentary Assembly or Common Assembly. It is the parliament of the EU. EU citizens elect its members once every five years. Together with the Council of Ministers, it is the lawmaking branch of the institutions of the Union. Additional information: http://simple.wikipedia.org/wiki/European_Parliament
Fair and Accurate Credit Transactions Act (FACT Act or FACTA)	U.S. Public Law 108-159, enacted in 2003 to amend the Fair Credit Reporting Act with the purpose of preventing identity theft, improving resolution of consumer disputes, improving the accuracy of consumer records, and making improvements in the use of and consumer access to credit information. ARMA Glossary 2012
Family Educational Rights and Privacy Act (FERPA)	U.S. statute (20 U.S.C. § 1232g; 34 CFR Part 99), enacted in 1974 to protect student and parent rights to access the student's records kept by the school, and to restrict access to those records by others without the permission of the student or parents. ARMA Glossary 2012
Federal Rules of Civil Procedure	The regulations that specify procedures for civil legal suit within U.S. federal courts. ARMA Glossary 2012
Federal Trade Commission (FTC)	A bipartisan federal agency with a unique dual mission to protect consumers and promote competition. Additional information: https://www.ftc.gov/about-ftc/what-we-do
General Data Protection Regulation (GDPR)	A single law by the European Commission that unifies data protection within the European Union. Additional information: https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Generally Accepted Recordkeeping Principles (the Principles)	A framework of definitive principles for governing an organization's information as a strategic asset. These information governance principles support organizational goals, facilitate compliance with the regulatory, legislative, and information management requirements and limit risks. Note: Established by ARMA International in 2009, the principles were synthesized from authoritative international and national standards and global best practice resources for governing information. ARMA Glossary 2012
Health Information Technology for Economic and Clinical Health Act (HITECH)	Promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules. Additional information: http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
Health Insurance Portability and Accountability Act (HIPAA)	U.S. Public Law 104-191, enacted in 1996, that addresses the use of individuals' protected health information by organizations that are subject to the Standards for Privacy of Individually Identifiable Health Information. Its goal is to allow for the exchange of information needed to provide high-quality health care while protecting patient privacy. ARMA Glossary 2012
Information Commissioner's Office	The Information Commissioner's Office (ICO) is an independent authority in the UK that promotes openness of official information and protection of private information. According to its web site, the ICO does this "by promoting good practice, ruling on eligible complaints, providing information to individuals and organizations, and taking appropriate action when the law is broken." The ICO oversees: 1) The Data Protection Act; 2) the Freedom of Information Act; 3) the Environmental Information Regulations, and 4) the Privacy and Electronic Communications Regulations. Additional information: http://searchstorage.techtarget.co.uk/definition/Information-Commissioners-Office-ICO
International Data Transfer	The transfer of any type of personal information to countries or international or supranational entities that do not provide adequate levels of protection (adequate protection levels may arise from contractual clauses or other means) is prohibited. Additional information: http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf
International Principles for the Application of Human Right to Communication Surveillance (Mexico)	13 principles about limiting surveillance. They are endorsed by the Mexican Federal District data protection authority (InfoDF) of the International Principles for the Application of Human Rights to Communications Surveillance. They are guidelines for cooperation between government and internet service providers and are one step toward the implementation of data retention mandate laws. Additional information: https://www.eff.org/deeplinks/2015/01/data-privacy-day-mexico-citys-privacy-authority-leads-latin-america-signing-13
Internet Traffic in Arms Regulations (ITAR)	A United States export control law that affects the manufacturing, sales and distribution of technology. Additional information: http://whatis.techtarget.com/definition/ITAR-and-EAR-compliance
ISO 9000	A series of standards developed and published by the International Organization for Standardization (ISO) that define, establish, and maintain an effective quality assurance system for manufacturing and service industries. Additional information: http://searchdatacenter.techtarget.com/definition/ISO-9000

ISO/IEC 29100	Provides a privacy framework which 1) specifies a common privacy terminology; 2) defines the actors and their roles in processing personally identifiable information (PII); 3) describes privacy safeguarding considerations, and 4) provides references to known privacy principles for information technology. It is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information or communication technology systems or services where privacy controls are required for the processing of PII. Additional information: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=45123
ISO/IEC 27018:2014	Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect personally identifiable information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment. Additional information: http://www.iso.org/iso/catalogue_detail?csnumber=61498
Italy's Law 231 (Anti-Corruption Law)	Italian legislation under Italian criminal corporate law that deems a company is considered criminally liable when the top management of the company, or the company's employees commit for the benefit of the company, certain criminal offenses listed in Law 231 (e.g. crimes of public and private corruption). Under this rule a company can be exonerated from liability in certain cases. Additional information: http://www.ethic-intelligence.com/experts/351-how-italy-has-toughened-its-anti-corruption-laws-and-what-this-means-for-companies/
Legal Services Act (LSA)	The Legal Services Act 2007 is an act of the Parliament of the United Kingdom that seeks to liberalize and regulate the market for legal services in England and Wales, to encourage more competition and to provide a new route for consumer complaints. It also makes provisions about the Legal Profession and Legal Aid (Scotland) Act 2007. Additional information: https://en.wikipedia.org/wiki/Legal_Services_Act_2007
NY Code - Article 6-A Personal Privacy Protection Law	New York State enacted the Personal Privacy Protection Law (Public Officers Law, Article 6-A, sections 91-99) in 1984 to recognize public concern about privacy and the relationship between government and the people. The law is intended to protect your privacy by regulating the manner in which the state collects, maintains and disseminates personal information about you. Generally, the law: 1) grants rights of access to you for records about you that are maintained by state agencies; 2) permits you to correct or amend information if you believe that it is inaccurate or irrelevant; 3) prohibits an agency from collecting personal information, unless it is relevant and necessary to a purpose of the agency that must be accomplished by law; 4) requires an agency, when it seeks personal information from you, to tell you why the information is being collected, where it will be kept, how it will be used, and what penalties, if any, may be imposed if you fail to provide the information; 5) protects you against disclosures of personal information without your consent, except in circumstances specified in the law; and forbids state agencies from maintaining secret data banks containing personal information. Additional information: http://www.dos.ny.gov/coog/shldno1.html
Organization for Economic Cooperation and Development (OECD)	The Organization for Economic Cooperation and Development (OECD) is a unique forum where the governments of 34 democracies with market economies work with each other, as well as with more than 70 non-member economies to promote economic growth, prosperity, and sustainable development. The Organization provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and coordinate domestic and international policies. The OECD helps countries – both members and non-members – reap the benefits and confront the challenges of a global economy by promoting sound energy policies that further economic growth; energy security; free markets; the increasingly safe, clean, and efficient use of resources to reduce environmental impacts and preserve our climate; and science and technology innovation. Additional information: http://usoecd.usmission.gov/mission/overview.html

PATRIOT Act	An Act of Congress signed into law on October 26, 2001 and stands for United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. It addresses such topics as: 1) enhancing domestic security against terrorism; 2) surveillance procedures; 3) anti-money laundering to prevent terrorism; 4) border security; 5) removing obstacles to investigating terrorism; 6) victims and families of victims of terrorism; 7) increased information sharing for critical infrastructure protection; 8) terrorism criminal law, and; 9) improved intelligence. Additional information: https://en.wikipedia.org/wiki/Patriot_Act
Privacy (types)	**Self-Regulatory:** refers to stakeholder-based models for ensuring privacy. The term self-regulation can refer to any or all of three pieces: legislation, enforcement and adjudication. Legislation refers to the question of who defines privacy rules. For self-regulation, this typically occurs through the privacy policy of a company or other entity, or by an industry association. Enforcement refers to the question of who should initiate enforcement action. Actions may be brought by data protection authorities, other government agencies, industry code enforcement or, in some cases, the affected individuals. Finally, adjudication refers to the question of who should decide whether an organization has violated a privacy rule. The decision maker can be an industry association, a government agency or a judicial officer. These examples illustrate that the term self-regulation covers a broad range of institutional arrangements. For a clear understanding of data privacy responsibilities, privacy professionals should consider who defines the requirements, which organization brings enforcement action and who actually makes the judicial decisions. **Co-Regulatory:** emphasizes industry development of enforceable code or standards for privacy and data protection against the backdrop of legal requirements by the government. Co-regulation can exist under both comprehensive and sectorial models. **Sectorial:** laws that exist only in areas where the legislative body has found a particular need. **Comprehensive:** laws that govern the collection, use and dissemination of personal information in the public and private sectors (e.g. Omnibus Laws). Additional information: https://privacyassociation.org/resources/glossary#self-regulatory-model
Privacy Act of 1974	The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Additional information: http://www.justice.gov/opcl/privacy-act-1974
Privacy by Design (PbD)	Privacy by Design is an approach to systems engineering which takes privacy into account throughout the whole software engineering process. The concept is an example of value sensitive design, (i.e., to take human values into account in a well-defined matter throughout the whole process) and may have been originally derived from this. The concept originates in a joint report on "Privacy-enhancing technologies " by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organization for Applied Scientific Research in 1995. The Information & Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian, has marketed the concept of Privacy by Design since the late 1990s. Additional information: https://en.wikipedia.org/wiki/Privacy_by_design
Privacy Enforcement (PE) Authorities	Associated with an APEC Cross-border Privacy Enforcement Arrangement (CPEA), a PE Authority is any public body that is responsible for enforcing information privacy law, and that has powers to conduct investigations or pursue enforcement proceedings. It can be a national or sub-national authority. Privacy Law is defined in the CPEA as the laws and regulations of an APEC economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework. Additional information: http://www.apec.org/

Sanctions	In civil law, a sanction is a part of a law that assigns a penalty for violation of the law's provisions. Additional information: http://legal-dictionary.thefreedictionary.com/sanction
Sarbanes-Oxley Act (SOX)	U.S. Public Law 107-204, enacted in 2002, that set new or enhanced standards for corporate auditing and accountability. ARMA Glossary 2012
Solicitor Regulation Authority (SRA)	The Solicitors Regulation Authority (SRA) is the regulatory body for solicitors in England and Wales. It is responsible for regulating the professional conduct of more than 125,000 solicitors and other authorized individuals at more than 11,000 firms, as well as those working in-house at private and public sector organizations. The SRA was formed in January 2007 by the Legal Services Act to serve as the independent regulatory arm of the Law Society. In a report by Sir David Clementi of all legal services in England and Wales, he recommended that professional bodies holding both regulatory and representative responsibilities should separate those roles. The Law Society remains the representative body for solicitors. Additional information: https://en.wikipedia.org/wiki/Solicitors_Regulation_Authority
UK Anti-Bribery Law	A UK law that makes it illegal to offer, promise, give, request, agree, receive or accept bribes. Additional information: https://www.gov.uk/anti-bribery-policy
UN Universal Declaration of Human Rights	A declaration adopted by the United Nations General Assembly. The goal was to represent the global expression of rights to which all human beings are inherently entitled. Additional information: https://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights
US Customs and Border Protection Regulations	Regulations established by the US Customs and Border Protection that govern the return of US citizens from abroad, residence and international visitors to the United States. Additional information: http://www.cbp.gov/travel/us-citizens/CBP-declaration-form-6059B
US Foreign Corrupt Practices Act (FCPA)	The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. (FCPA), was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. Specifically, the anti-bribery provisions of the FCPA prohibit the willful use of the mails or any means of instrumentality of interstate commerce corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person. Additional information: http://www.justice.gov/criminal/fraud/fcpa/
US Intelligence Reform & Terrorism Prevention Act of 2004 (IRTPA)	The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) is an Act of Congress that broadly affects United States federal terrorism laws. In juxtaposition with the single-subject rule, the act is composed of several separate titles with varying subject issues. It addresses privacy and civil liberties. Additional information: https://en.wikipedia.org/wiki/Intelligence_Reform_and_Terrorism_Prevention_Act

APPENDIX B: DATA LAWS

OECD (Organization for Economic Co-operation and Development)
Guidelines governing the protection of privacy and trans-border flows of personal data (1980)
http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

EU DPD (European Union Data Protection Directive) for data to travel freely between countries with adequate protection (1995 & 2012)
http://ec.europa.eu/justice/data-protection/

Article 29 Working Party
DPD group for the EU and European Commission
https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29

APEC (Asia-Pacific Economic Cooperation) Privacy Framework (2004)
http://www.apec.org/Home/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group

PIPEDA (Canadian Personal Information Protection and Electronic Documents Act)
https://www.priv.gc.ca/leg_c/r_o_p_e.asp

UK Anti-Bribery Law
https://www.gov.uk/anti-bribery-policy

In the US:

FRCP (Federal Rules of Civil Procedure)
https://www.law.cornell.edu/rules/frcp

HIPAA
http://www.hhs.gov/ocr/privacy/

HITECH
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

Fair Credit Reporting Act
https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act

Electronic Communication Privacy Act
https://epic.org/privacy/ecpa/

Gramm-Leach Bliley Act
https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

COPPA (Children's Online Privacy Protection Act)
http://www.coppa.org/

Privacy Act of 1974
http://www.justice.gov/opcl/privacy-act-1974

Freedom of Information Act
http://www.foia.gov/

CAN-SPAM Act
https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

Dodd-Frank Act
http://www.cftc.gov/lawregulation/doddfrankact/index.htm

FERPA (Family Educational Rights and Privacy Act)
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

FCPA (US Foreign Corrupt Practices Act)
https://www.sec.gov/spotlight/fcpa.shtml

REFERENCES

1 Law Firm Information Governance Symposium. (2012, August). *A Proposed Law Firm Information Governance Framework*. Retrieved from http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/White-Papers-Briefs/A/A-Proposed-Law-Firm-Information-Governance-Framework.aspx

2 Council of Bars and Law Societies of Europe. (2008, January 31). *Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers*. Retrieved from http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_CCBE_CoCpdf1_1382973057.pdf

3 dlapiperdataprotection.com. (n.d.). Retrieved June 12, 2015, from http://www.dlapiperdataprotection.com/#handbook

4 ARMA International. (2014). *Generally Accepted Recordkeeping Principles*. Retrieved from http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles

5 Cavoukian, A. (2011, January). *Privacy by Design: The 7 Foundational Principles*. Retrieved from https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

6 Cavoukian, A. & Chanliau, M. (2013, January). *Privacy and Security by Design: A Convergence of Paradigms*. Retrieved from https://www.ipc.on.ca/images/resources/pbd-convergenceofparadigms.pdf

7 Organization for Economic Co-Operation and Development. (2007) *Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*. Retrieved from http://acts.oecd.org/Instruments/ShowInstrumentView.aspx?InstrumentID=119&InstrumentPID=115&Lang=en&Book=

8 European Commission. (n.d.). *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*. Retrieved from http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf

9 Hogan Lovells. (2014, December 19). *Russian Data Localization Law May Now Come into Force One Year Ahead of Schedule, in September 2015*. Retrieved from http://www.hldataprotection.com/2014/12/articles/international-eu-privacy/russian-data-localization-law-may-now-come-into-force-one-year-ahead-of-schedule-in-september-2015/

10 Richardson, J. G. (2013, August). *Use Caution When Traveling With Encryption Software*. Retrieved from http://www.nationaldefensemagazine.org/archive/2013/August/pages/UseCautionWhenTravelingWithEncryptionSoftware.aspx

11 U.S. Department of State. (n.d.). *Passports and International Travel Alerts and Warnings*. Retrieved June 12, 2015 from http://travel.state.gov/content/passports/english/alertswarnings.html

BIBLIOGRAPHY

Koti, I. (2014). *The Cultural Implications of Information Governance – Why One Size Does Not Fit All in a Global Society*. Retrieved from http://www.2-20rm.com/blog/the-cultural-implications-of-information-governance-why-one-size-on-size-does-not-fit-all-in-a-global-society/

PROFESSIONAL ETHICS

Code of Conduct for European Lawyers
http://www.ccbe.eu/index.php?id=32

Charter of Core Principles of the European Legal Profession
http://www.ccbe.eu/fileadmin/user_upload/NTCdocument/EN_CCBE_CoCpdf1_1382973057.pdf

International Association of Lawyers
A non-exhaustive database containing "the fundamental documents that govern and structure the legal profession, such as charters, laws, ethics codes and documents."
http://www.uianet.org/en/documentation/profession

Rules of Professional Practice (Germany)
http://www.brak.de/w/files/02_fuer_anwaelte/berufsrecht/bora_engl_stand_1_11_2011.pdf

Solicitor Regulatory Authority (SRA) of the Law Society of England and Wales
http://www.sra.org.uk/handbook/

The Council of Bars and Law Societies of Europe (CCBE)
http://www.ccbe.eu/

DATA PRIVACY AND TRANSFER

Baker & McKenzie's 2013 Global Privacy and Information Management Handbook
http://www.bakermckenzie.com/files/Uploads/Documents/North%20America/DoingBusinessGuide/Houston/bk_globalprivacyhandbook_13.pdf

Diamond, M. (2014, July 29). *Preparing for the EU 2015 Data Protection Rules: What You Need To Know*. Webinar. Retrieved from https://www.youtube.com/watch?v=TUvwvXwkPfg

Generally Accepted Privacy Principles (GAPP)
http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf

Generally Accepted Recordkeeping Principles (The Principles)
http://www.arma.org/docs/bookstore/theprinciplesmaturitymodel.pdf

Global Internet Liberty Campaign. (n.d.). *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. Retrieved from http://gilc.org/privacy/survey/intro.html

Hunton & Williams LLP's Privacy and Information Security Law Blog
https://www.huntonprivacyblog.com/tag/data-transfer/

International Association of Privacy Professionals (IAPP) News
https://privacyassociation.org/news

International Privacy Laws
http://www.informationshield.com/intprivacylaws.html

Koti, I. (2014). *Integrating Privacy into the Information Governance Landscape*. Presentation at InfoGovCon 2014. Retrieved from https://www.youtube.com/watch?v=3vZ_Bej3Aio

Perspecsys. (n.d.). *German Data Privacy Laws*. Retrieved from http://perspecsys.com/how-we-help/cloud-privacy/german-data-privacy-law/

Privacy and Security by Design: A Convergence of Paradigms
https://www.ipc.on.ca/images/resources/pbd-convergenceofparadigms.pdf

US Privacy Laws
http://www.informationshield.com/usprivacylaws.html

Wessing, T. (2013, January). *A German perspective on International Data Transfers*. Retrieved from http://www.taylorwessing.com/globaldatahub/article_data_transfers_germany.html

INFORMATION/DEVICE MOBILITY

Overseas Security Advisory Council
https://www.osac.gov/Pages/Home.aspx

U.S. Department of Justice, Federal Bureau of Investigation
https://www.fbi.gov/

U.S. Department of State, Travel Alerts and Warnings
http://travel.state.gov/content/passports/english/alertswarnings.html

RETENTION

De Brau Blackstone Westbroek. (2014, October). *European Document Retention Guide: A Comparative View Across 16 Countries to Help You Better Understand Legal Requirement and Records Management Best Practice*. Retrieved from http://www.debrauw.com/wp-content/uploads/2015/01/EU-Retention-Guide-2014.pdf

Saffody, W. (2014). *Legal Requirements for Electronic Records Retention in France*. For purchase. Retrieved from https://members.arma.org/eweb/browse.aspx?site=armastore&webcode=product&id=e5b5c9a9-0787-4ff0-b77b-28a695abc846#.VXsYf09VhHw

Saffody, W. (2014). *Legal Requirements for Electronic Records Retention in Germany*. For purchase. Retrieved from https://members.arma.org/eweb/browse.aspx?site=armastore&webcode=product&id=18c1b2a2-59fa-4d2b-bad4-18ded08b9ef9#.VXsaWE9VhHw

Saffody, W. (2014). *Legal Requirements for Electronic Records Retention in Italy*. For purchase. Retrieved from https://members.arma.org/eweb/browse.aspx?site=armastore&webcode=product&id=6ac7cfc4-6412-4d6c-9108-001fed298248#.VXsY2U9VhHw

Saffody, W. (2014). *Legal Requirements for Electronic Records Retention in United Kingdom*. For purchase. Retrieved from https://members.arma.org/eweb/browse.aspx?site=armastore&webcode=product&id=f4049283-d737-45a5-89ca-520ff8cf92f9#.VXsYzU9VhHw

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM) provides information management services that help organizations lower the costs, risks and inefficiencies of managing their physical and digital data. Founded in 1951, Iron Mountain manages billions of information assets, including backup and archival data, electronic records, document imaging, business records, secure shredding, and more, for organizations around the world. Visit the company website at www.ironmountain.com for more information.

US-LAW-EXT-BR-080715-001