ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Challenges for Corporate Counsel When Facing Cross-Border Discovery and Investigation Requests

Compliance and Ethics

Technology, Privacy, and eCommerce


MONGOLIA
GOBI
CHINA
Urumqi
Yinchuan
Hohhot
Beijing
Changchun
Zhengzhou
Shanghai
Wuhan
Nanchang
Taipei
TAIWAN
Yumen
Xi'an
Chengdu
Chongqing
Xiamen
Guiyang
Kunming
Macau
Hong Kong
HAINAN
Hotan
Lhasa
BHUTAN
NEPAL
Islamabad
Hanoi
VIETNAM
Manila
LUZON
PHILIPPINE SEA
BANGLADESH
MYANMAR
LAOS
New Delhi
Jabalpur
Kolkata
Nay Pyi Taw
THAILAND
SOUTH CHINA SEA
INDIA
Yangon
Bangkok
CAMBODIA
Hyderabad
BAY OF BENGAL
MALAYSIA
BRUNEI
SINGAPORE
Mumbai
ARABIAN SEA
PAKISTAN
AFGHANISTAN
TAJIKISTAN
KYRGYZSTAN
KAZAKHSTAN
RUSSIA

Technology today allows information to travel at the speed of business — and makes “borders” as we historically knew them, meaningless. Virtual teams and cross-functional collaboration are the norm, and the results have been extremely positive for business. Work can be done around the globe and around the clock with relative ease. Skills and experience, rather than geographic location, are the primary factors when assembling work teams. That all sounds great… except when the work performed by that geographically diverse, cross-functional team is needed to respond to a discovery request or regulatory investigative demand in the United States. The ever-growing, complex web of privacy protection laws around the world directly impacts how multinational corporations can comply with such demands. The risk of running afoul of privacy laws in the name of compliance with a US legal obligation is very real and often unanticipated. Knowing where the risks exist and crafting practical processes to both comply with US obligations and meet international privacy standards are some of the largest challenges facing the multinational corporation today. As with almost any legal risk, it is important to be prepared.

Why it matters

More than 70 countries around the world currently have privacy laws in place, yet there are differing requirements and penalties imposed for violations. The stakes are high: Violations can carry severe

penalties, both civil and criminal. Depending on the country, these sanctions may take the form of fines or imprisonment. Noncompliant companies and their officers and directors face potential personal criminal liability, even if the violation was unintentional. For example, if the current draft of the European General Data Protection Regulation becomes effective in early 2016 as anticipated, it will provide for potential business fines of up to two percent of annual income. Noncompliance therefore poses a material risk to any company, and its executives, subject to the regulation. So what can counsel do to best mitigate this risk?

Be prepared — Know what data is where

Before the urgency of an active request hits, in-house counsel can help mitigate the risk of a privacy violation by understanding where the corporation “keeps” all the critical business data. This “data map” will set out the different kinds of systems that exist in the corporation and indicate where key business functions are performed. Armed with this information, counsel can begin to consider the potential cross-border implications of a request. Creating a data map used to be a relatively simple endeavor. However, determining “where” data resides has become a more complex inquiry, with more and more companies consolidating data centers, outsourcing and using cloud storage. For example, counsel at a car manufacturer selling cars in the United States needs to know that a component part of one of its models was designed and manufactured in Germany, and therefore much of the information about that part likely exists and is stored in Germany.

Similarly, if a company has outsourced its back office financial functions to China, counsel can proactively examine Chinese state secret and privacy requirements, which would allow counsel to make an effective plan for producing that information when it is needed for an investigation or litigation.

Geographic borders are meaningless

At first blush, the issues of cross-border transfer and privacy seem to be in relative harmony. If you know where the data is and the data is in a jurisdiction which affords it privacy protection and/or restricts cross-border transfer, the result seems simple: You cannot collect or move the data without appropriate privacy law compliance. Think again. In a hotly contested dispute currently pending before the Second Circuit Court of Appeals, Microsoft was ordered to produce a Hotmail user’s emails that were stored on a server in Dublin, Ireland, a country subject to and a part of the 1995 European Union Data Protection Directive (the “Directive”). US Magistrate Judge James C. Francis of the Southern District of New York ruled that Microsoft must hand over a user’s emails stored on a server in Dublin to federal prosecutors. Judge Francis ruled that as long as a company remains in control of the data, access to that data does not require the physical ability to walk into a data center to see the data servers. Instead, access to data transcends borders: If a company has the “practical ability” to collect the data, even if the server resides outside the United States, then the data is not beyond the reach of the United States government. This has very real implications to the corporate IT organization that routinely builds in “back door” access to international systems for purposes of global management and software deployment. Even if not readily apparent, that back door access, under current Microsoft precedent, can be the basis for requiring the company to violate data privacy laws. US District Judge Preska upheld Judge Francis’ order and the matter is currently scheduled for oral argument before the Second Circuit on September 9, 2015. The outcome of the *Microsoft* decision will greatly impact not only the transfer of data cross-border, but potentially the way that corporations organize their global business and information functions.

Practical steps toward compliance

So what does this mean for the business? Without unequivocal direction from the courts, the struggle to balance the risk of privacy violation against the risk of non-compliance becomes an exercise in reasonableness. But all hope is not lost. Incorporating the following considerations into your response plan can help mitigate risk:

1. Seek statutory or procedural protections. If the results of your data mapping exercise show that information likely to be needed to respond to a litigation or regulatory demand is stored in a jurisdiction affording privacy protection to personal information of your workers, consider seeking Safe Harbor Certification, using binding corporate resolutions or standard contractual clauses to demonstrate the protection required if the personal information must be transferred. On a case-specific basis, use the model protective order provisions recommended by the Sedona Conference.
2. Procedurally, establish a process that will allow the company to demonstrate compliance with the major privacy principles:
   a. Legitimate purpose: Document the valid business purpose for the transfer of personal data;
   b. Notice: Inform individuals that their data is being collected and detail how the data will be used;
   c. Opt out: Provide individuals with the option to opt out of the collection or transfer of the data;
   d. Onward transfer: If your case requires transfer of data to third parties, ensure that those third parties also follow adequate data-protection principles; and
   e. Security: Once transferred, ensure that your IT infrastructure has adequate safeguards against the loss or breach of collected information.
3. Work local, think global. If possible, once consent or other required “collection” requirements have been met, work in-country to narrow any collected dataset to that which is most likely to be responsive to the request. This can take several forms; from full processing and review for responsive information in-country and export of only responsive information, to basic culling and personal information screening in-country prior to export. The key to selecting the correct protocol for your case will require close collaboration with your counsel and technology consultant. Understanding all your technology options will help ensure that your organization is not incurring avoidable risk. There are many technological approaches, from simple culling to advanced predictive coding analytics, which can be applied in-country to get to the most likely responsive information. These efforts can considerably reduce the dataset to be transferred.
4. Consider phased discovery. Be sure to explain to any court or regulator seeking cross-border discovery of personal information that certain procedural steps will be necessary for you to comply with the request. Set appropriate expectations for timing, which might involve phasing production with non-protected data first and protected data in a subsequent phase.
5. Cultivate a culture of compliance. As in any defense of corporate conduct, you will be more effective at persuading courts, data protection agencies and regulators that the company respects and intended to comply with all applicable laws and regulations if you can demonstrate that compliance is top of mind, both in process and policy.

Conclusion

For today’s global corporation, retreating within national boundaries or failing to meet production requirements is simply not an option. But the challenges in balancing production requirements and

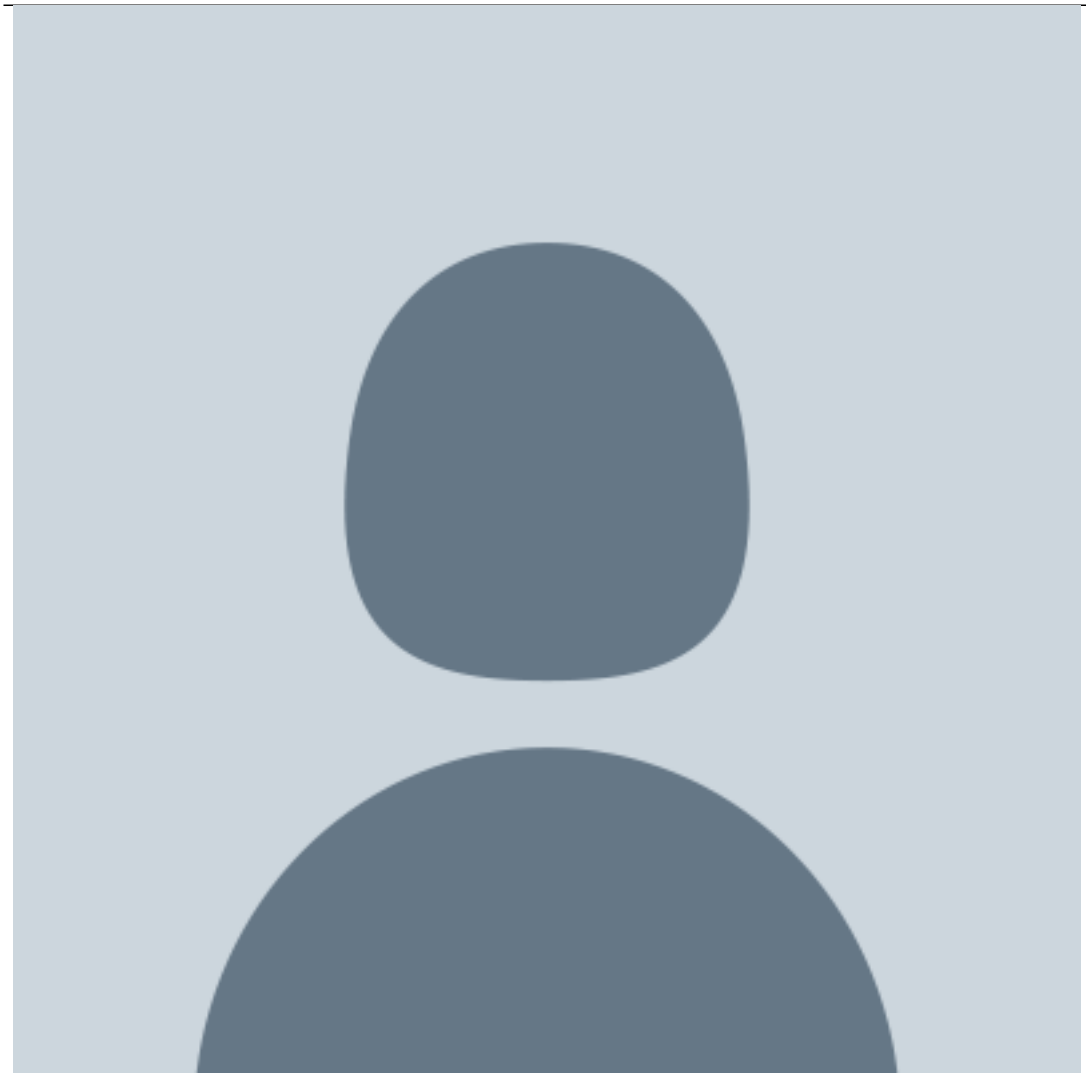
privacy compliance, while large, are not insurmountable. With some advance planning and strategic advisors, every company can successfully navigate data protection waters while maintaining the efficiencies and synergies gained through global collaboration.

Notes

1 The Directive regulates the processing of personal data, defines baseline requirements for companies possessing the personal data, and specifies what can or cannot be done with that data, including cross-border transfer. Assuming a valid business purpose or specific exception, data can be transferred only to countries that afford an adequate level of privacy protection, as in the home country. Although the US has some legislation offering privacy protection, these measures have been deemed “not adequate protection” by the European Union and other countries. To navigate around this impediment, the US Department of Commerce and the European Commission developed the safe-harbor framework, through which companies could demonstrate voluntary adherence to an adequate privacy-protection standard, or companies can demonstrate adequate protection by the use of binding corporate resolutions or standard contract clauses. Outside the EU, several other countries are enacting or amending their existing privacy laws to provide for similar administrative hurdles to transfer. As an example, in Japan, the Personal Data Protection Act (“PDPA”) defines personal information as any information that can identify a living individual. This definition is intentionally broad and would include even publicly available information. Any mechanism that allows this information to be collected, organized, searched or otherwise easily retrieved is classified as a Personal Information Database. Any entity that uses such a database is subject to the requirements set out by the PDPA. The entity must make a public announcement of the use of the data, and consent must be obtained for any use outside of that announcement. There is a general prohibition against sharing data with third parties—including affiliated entities—except in very limited circumstances. The security and integrity of the personal data must also be protected at all times. Breaches of the PDPA can result in both criminal and civil penalties. In the last five years, Singapore, Malaysia, the Philippines, South Korea and Taiwan have also passed their respective data privacy laws, and Thailand is currently in the drafting stage In Brazil, a new Data Protection Bill has just entered public debate. If passed into law, the Bill would bring Brazil’s data protection regime more in line with that of the EU. In other countries, laws are on the books that provide stringent nominal protections.

2 See also The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in US Litigation.

Elizabeth Erickson



UBIC, Inc.