Issues in Accessing Foreign Personal Information for Use in US Legal Proceedings

By Jeane Thomas, JD

Imagine your organization is involved in a lawsuit or government investigation and needs to access documents or information located outside the United States. If you think you can just demand that they be sent to the US because they are relevant or maybe even necessary for the legal matter—not so fast.

For companies involved in litigation in the US, the production of confidential information relevant to the case—including personal health information—is commonplace. American entities deal with the confidentiality concerns by producing such information subject to protective orders and non-disclosure agreements that allow parties to use the information for purposes of the litigation, but prevent it from being misused for other means.

The US discovery regime is extremely broad, allowing parties to demand all documents and information relevant to their claims and defenses. It is no excuse to assert that the information called for is personal or sensitive. Further, parties have an obligation to turn over information in their "possession, custody or control," and employees, customers, or other third parties have virtually no ability to control what the organizations that maintain their personal information do with that information when they are required to produce it for legal proceedings.

But the situation is very different in many countries outside of the US, most notably in the European Union (EU) and the dozens of other countries that follow an EU-style approach to data protection. Within the EU, the ability of every citizen to control what happens with his or her personal information is considered a fundamental human right. Accordingly, laws within the EU grant specific data protection rights to individuals and prevent organizations that control data from processing or transferring personal data except under certain conditions.

Personal information is defined broadly to include "any information relating to an identified or identifiable natural person." In other words, personal information is anything that allows anyone to link information to a specific person. Examples include physical or e-mail addresses, phone numbers, bank information, video images, and, of course, health information. Because these rights belong to individuals, they exist without regard to where personal data about them is located, including information within the custody of their employers, third party e-mail, social media providers, healthcare providers, or insurers.

Competing Legal Obligations

This difference in approaches between jurisdictions creates very difficult conflicts when it comes to providing or obtaining personal information of non-US residents for use in US litigation or investigations. For example, consider a situation in which the health information of non-US residents is relevant to litigation in the US. Under our discovery rules, such information must be produced as long as it is relevant and within the possession, custody, or control of any party within the court's jurisdiction, such as an employer, healthcare provider, or research organization.

However, the production of such information in US legal proceedings may violate foreign data protection laws, which protect the rights of individuals who typically are not party to the litigation. Companies in this situation are caught between the proverbial rock and a hard place. They must choose between disobeying US discovery obligations and potentially violating a court order to produce such information on the one hand, or violating foreign law with potential criminal and/or financial penalties on the other hand.

Unfortunately, there is no straightforward process for harmonizing these conflicting legal obligations, and US courts have not shown much sympathy for parties dealing with these issues. The US Supreme Court addressed this type of conflict more than 25 years ago in the *Aérospatiale* case, which held that principles of international comity require an evaluation of the respective

interests of the US courts and the foreign nation whose laws are at issue. The Supreme Court set forth the factors relevant to the "comity analysis" that courts should apply when considering how to proceed with respect to non-US discovery:

1. The importance to the… litigation of the documents or other information requested
2. The degree of specificity of the request
3. Whether the information originated in the United States
4. The availability of alternative means of securing the information
5. The extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located

Following *Aérospatiale*, nearly every US court that has dealt with these cross-border discovery issues has decided that US interests in requiring litigants to meet their discovery obligations outweigh foreign interests in protecting the privacy interests of their citizens. These courts have ordered parties to comply with discovery requests and orders, notwithstanding the fact that such compliance would violate foreign law, in part because the courts have found that the risk of prosecution or penalty in the foreign jurisdictions is relatively low.

For example, a court in New York recently considered the extent to which foreign laws prohibiting the release of banking information, sometimes on pain of criminal prosecution, outweighed the need to produce the information in the US litigation. Asking the question, "But is this for real?" the court found that "the extent to which the relevant country has actually enforced the prohibition is a strong indicator of the strength of the state interest" and ordered the production of the information in *Motorola Credit Corp. v. Uzan*, 2014 WL 7269724 (S.D.N.Y., 2014).

Litigation Complications Will Persist

The difficulties for US litigants may become even more acute if the EU passes proposed data protection legislation that significantly increases the penalties for violation, possibly up to two percent of worldwide turnover per infraction. In addition, with China and other countries passing new data protection laws, or adding more teeth to existing regulations, the conflict with US-style discovery obligations is truly becoming a global issue. It remains to be seen how and when these conflicts ultimately will play out, but with the increasing volume of non-US information relevant to US litigation—along with increasing data protection enforcement around the world—it is certain that the issues will not go away anytime soon.

Jeane Thomas (jthomas@crowell.com) is a partner at the international law firm Crowell and Moring, LLP, based in Washington, DC.

Article citation:
Thomas, Jeane. "Issues in Accessing Foreign Personal Information for Use in US Legal Proceedings" *Journal of AHIMA* 86, no.4 (April 2015): 42-43.