ABA Antitrust Section | Global Private Litigation Committee

Global Private Litigation Bulletin

ABA SECTION OF ANTITRUST LAW

Promoting Competition Protecting Consumers

ISSUE 11 | March 2018

DARE TO SHARE? WAIVER ISSUES IN CROSS-BORDER JOINT DEFENSE COMMUNICATIONS

Christopher B. Hockett, Partner, Joshua S. Cohn, Associate, and Jonathan A. Huberman, Associate, Davis Polk & Wardwell LLP

Most U.S. lawyers know very little about foreign laws governing the attorney-client privilege or work product doctrine. However, ignoring those laws might, in certain circumstances, make confidential cross-border joint defense communications vulnerable to a claim of waiver, even in a U.S. proceeding. This article explains these risks, and offers some suggestions for mitigating them.

Information Sharing Under the Joint Defense Doctrine

Under U.S. law, the attorney-client privilege bars discovery of confidential communications between a client and counsel made in connection with obtaining or providing legal advice.[1] The privilege exists to encourage open communication between the attorney and client, a cornerstone of effective representation.[2] However, if an otherwise privileged communication is shared with strangers to the attorney-client relationship, then courts are likely to find a waiver of the privilege.[3] Similarly, an attorney's work product – material prepared in anticipation of litigation – should also be kept confidential to remain protected from discovery, although work product protection is not as easily waived by disclosure to outsiders.[4]

The joint defense or "common interest" doctrine is a widely – though not universally – recognized extension of the attorney-client privilege and work product doctrine.[5] Although the doctrine varies from jurisdiction to jurisdiction, in general it provides a mechanism for clients and lawyers to share privileged information with third parties that share a common interest without causing a waiver of otherwise applicable legal privileges.[6] A key requirement of an effective joint defense agreement is that it bars participants from disclosing confidential information received from others pursuant to the agreement.[7]

It is extremely common for joint defense groups in price-fixing matters to rely on common interest agreements to protect confidential communications and information shared among participants. These efforts help parties coordinate their defenses and design effective strategies in response to price-fixing claims and investigations – which frequently involve companies, counsel and enforcement agencies located in many different jurisdictions around the world.

However, some jurisdictions outside of the U.S. do not recognize the joint defense doctrine, or provide the same high level of protection for attorney-client communications or work product as under U.S. law. What, then, happens when joint defense information is shared with participants located in jurisdictions like these? Even if the information is shared in confidence pursuant to a joint defense agreement that prohibits its disclosure, is it reasonable for the sharing party to rely on privileges and non-disclosure promises that the receiving parties' jurisdictions would not uphold? If not, could sharing such information waive otherwise applicable privileges, even as interpreted by U.S. courts under U.S. law?

Foreign Privilege Law

It is beyond the scope of this article to address all of the variations in the law of privilege in non-U.S. jurisdictions.[8] However, there are many important jurisdictions that afford significantly less protection for attorney-client communications and attorney work product than does U.S. law. The EU, for example, recognizes a "legal professional privilege," which allows a party under investigation by the European Commission to withhold communications with an external lawyer who is qualified to practice in a member state within the European Economic Area in relation to the subject-matter of that investigation (even if the advice was provided prior to commencement of the investigation). However, legal professional privilege does not attach to an internal communication between an in-house counsel and the company, unless it merely reports advice provided by an external lawyer which is privileged, nor does it attach to communications with non-EU-qualified counsel. There is also an open question as to whether EU courts would recognize the common interest privilege. China, meanwhile, affords even less protection to attorney-client communications: while an attorney has a professional obligation to maintain the confidentiality of client information, she, along with "all work units and individuals that have knowledge of the circumstances of a case," can be required to "give testimony in court" and disclose that confidential information (and could face professional discipline or even jail time if she refuses to do so).[9]

As a result of these varying degrees of protection throughout different jurisdictions, there could be some risk in relying on U.S. law to protect confidential attorney-client communications, attorney work product, and joint defense material shared with joint defense participants located in multiple jurisdictions. One way that risk could manifest itself is if enforcement authorities or private litigants in the foreign jurisdictions were to compel disclosure of the shared joint defense information.[10] However, the risk could also arise in the context of a claim of privilege or work product waiver in a U.S. proceeding. That is our next topic.

The Analogy To Non-Private Email

Viewed broadly, the question is whether a privilege can be maintained with respect to communications or work product that is meant to be shared in confidence with joint defense participants, but which the sharing party knows, or should know, *might* be disclosed to adverse third parties in the future because those adverse third parties *might* (or already *do*) have access to the communication.

An analogous situation has arisen under U.S. law in the employment context, where an employee uses a company email account, or a company computer, to communicate with personal (i.e., non-corporate) counsel about an employment dispute. Virtually all U.S. companies have access to emails sent or received via their email exchanges, and are also able to access saved computer files. Moreover, many companies have policies in place expressly reserving the right to monitor employee email and computer use, including the contents of communications and files maintained on company systems. Accordingly, there have been a number of decisions finding that employees had no reasonable expectation of privacy with respect to their use of these systems.[11]

In the privilege context, employees' emails with their personal counsel have been sought in discovery by employers based on a claim of waiver. And although an employee using company computers to communicate with his or her personal attorney may have believed that the communications were privileged and confidential, that privilege claim does not always hold up.

The leading case is I*n re Asia Global Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005), which sets forth four factors for courts to consider in evaluating a claim of waiver in these circumstances: "(1) does the corporation

maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies."[12] In *Asia Global*, the court determined that the employee had not been informed of the company's monitoring policies and therefore had no reason to doubt that his communications with personal counsel were confidential; thus, he had not waived privilege by emailing on the company's system.[13]

Subsequently, however, a number of courts have followed *Asia Global*'s reasoning and decided that employees *had* waived privilege by using company systems that they knew, or had reason to know, were being monitored.[14] Indeed, the court in *In re Royce Homes, LP*, 449 B.R. 709 (Bankr. S.D. Tex. 2011), went so far as to find that using the company email system effected a waiver of the *entire subject matter* of the employee's communications, not merely a waiver as to the communications made with the company system.[15] As a result, a key employee in the bankruptcy proceeding was forced to disclose thousands of emails with his attorney.[16]

So, in the context of cross-border joint defense communications, is it objectively reasonable for a party to share joint defense information with foreign parties or counsel who cannot effectively assert attorney-client privilege or the work product doctrine to protect that information from disclosure to potential adversaries? And if not, could the rationale of *Asia Global* be applied in such cases to support a finding of waiver – in a U.S. court – of otherwise clearly applicable privileges and protections?

As explained below, we believe that the better argument is that a waiver should not be found in these circumstances. However, to our knowledge the issue has not been litigated, so the outcome is difficult to predict with certainty.

Asia Global and Waiver Issues in Cross-Border Joint Defense Communications

Below we review the relevant *Asia Global* factors[17] to see whether applying them could support a waiver argument regarding joint defense communications with unprotected foreign participants.

Notice: As noted at the outset of this article, most U.S. lawyers are not familiar with the privilege law of other countries, and thus might not have actual notice that some countries do not recognize the attorney-client privilege or work product doctrine. However, U.S. lawyers might reasonably be expected to know about privilege protections that apply (or do not apply) to the other members of their joint defense group. In other words, subjective ignorance of lowered protections may not be a sufficient excuse for lack of "notice."[18]

Monitoring and Access: In the employment context, an employer's ability to "monitor" an employee's computer or email use connotes ongoing or at-will inspection rights regarding the communications at issue.[19] Obviously, that sort of monitoring would be highly unusual in the joint defense context, as adversarial third parties such as enforcers or private litigants normally do not have regular access to those communication channels. Thus, even in countries with diminished privilege protections, hostile third parties would not have ongoing rights to inspect joint defense information.

However, the same adversaries could obtain "access" to joint defense communications by invoking their investigative or subpoena powers. Would the existence of that hypothetical right of access make sharing joint defense information vulnerable to a claim of waiver? At least some cases in the employment context suggest that waiver requires more than theoretical vulnerability to disclosure; if the right of access is not actually

exercised in practice, then some courts have been more willing to find that the employee enjoyed a reasonable expectation of privacy when using company systems, and thus that no waiver occurred.[20] In the context of joint defense communications, there would rarely be any ongoing monitoring or real-time access by adversaries, and obtaining access generally would require taking significant affirmative steps (e.g., through a subpoena or other compulsory process) to uncover the confidential information. Thus it seems incorrect to assume that merely sharing joint defense information with participants in countries that do not uphold privileges would necessarily destroy any reasonable expectation of privacy.

Moreover, a party might further protect against a claim of waiver by avoiding any voluntary production of the joint defense communications. In general, a party waives the attorney client privilege by voluntarily disclosing confidential communications to a third party that is not within the privilege.[21] This includes voluntary disclosures made to foreign regulators.[22] Compelled disclosures, on the other hand, do not constitute voluntary waivers to third parties, and therefore do not waive the attorney-client privilege.[23]

Mitigating the Risk

In the absence of clear law, there are a number of steps parties can take to reduce the likelihood that a U.S. court would find a waiver when joint defense information has been shared with participants in countries that do not recognize the same privileges and protections provided under U.S. law.

1. Limit the information that you share with people in vulnerable jurisdictions, especially those in in-house counsel roles. If a member of a joint defense group resides in a country that limits protections for in-house counsel, consider limiting any privileged communications or work product to the outside attorneys.

2. Clearly label privileged information. Marking information as privileged provides two benefits. First, clear privilege designations allow electronic systems to identify the documents and may help prevent inadvertent disclosure of the information. Second, because U.S. courts will consider whether the parties had a reasonable expectation of privacy, marking the joint defense information as privileged can help to establish that the parties took steps to maintain confidentiality of the documents.

3. Specify in the joint defense agreement that sharing information pursuant to its terms is not intended to waive any protections. Because U.S. courts will consider a party's reasonable expectations, a court may credit a contractual provision stating that the parties intend privileged information or work product to remain protected.

4. Require notice and opportunity to intervene if joint defense information is requested by any outsider. If a participant voluntarily discloses confidential joint defense information to a hostile third party (e.g., a foreign enforcer), a U.S. court is more likely to find a waiver. By contracting for the opportunity to object to any disclosure, joint defense group participants can limit their exposure to such a finding.

Conclusion

Members of cross-border JDA's should carefully evaluate the risks posed by sharing joint defense information with participants subject to less protective foreign privilege laws. Although the law is unsettled, parties should take steps to minimize these risks and avoid a waiver.

---

[1] RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (2000); *see also United States v. United Shoe Machinery Corp.*, 89 F. Supp. 357, 358 (D. Mass 1950).

[2] *Jaffee v. Redmond*, 518 U.S. 1, 11 (1996).

[3] *See, e.g., Westinghouse Electric Corp. v. Republic of the Philippines*, 951 F.2d 1414, 1424 (3d Cir. 1991).

[4] *Id.* at 1428*; see also Kraus Industries v. Moore*, 2008 WL 4206059, at *4 (W.D. Pa. Feb. 11, 2008).

[5] *See United States v. Schwimmer*, 892 F.2d 237, 243 (2d Cir. 1989).

[6] *See United States v. Hsia*, 81 F. Supp. 2d 7, 16 (D.D.C. 2000). As noted in Elizabeth Castillo's companion article in this newsletter, the doctrine does not confer an independent privilege; it merely prevents a waiver that would otherwise occur when privileged or work product-protected information is disclosed to third parties. Castillo, Elizabeth T., "Misconceptions About Privilege Relating to Everyday Agreements", at 4; *see also In re Grand Jury Subpoenas, 89-3 and 89-4*, 902 F.2d 244, 249 (4th Cir. 1990) ("[A]s an exception to waiver, the joint defense or common interest rule presupposes the existence of an otherwise valid privilege").

[7] *Western Fuels Ass'n v. Burlington Northern Railroad Co.*, 102 F.R.D. 201, 203 (D. Wyo. 1984).

[8] For more thorough discussion of these variations, we recommend the companion articles in this newsletter by Deba Das and Jessica Steele (England and Wales), Simon Priddis and Thomas Wilson (EU), Sabrina Protocic (Germany), Gian Luca Zampa and Mario Cistaro (Italy), and Winfred Knibbeler and Nima Lorjé (Netherlands).

[9] *See Wultz v. Bank of China Ltd.*, 979 F. Supp. 2d 479, 491 (S.D.N.Y. 2013), *aff'd in part rev'd in part on other grounds*, 2013 WL 6098484 (S.D.N.Y. Nov. 20, 2013).

[10] *See In re Vitamin Antitrust Litig.*, 2002 WL 35021999, at *4, *26 (D.D.C. Jan. 23, 2002).

[11] *See, e.g., Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 WL 974676 at *2 (D. Mass. May 7, 2002); *In re The Reserve Fund Sec. & Derivative Litigation*, 275 F.R.D. 154, 159-165 (S.D.N.Y. 2011); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996); *United States v. Simons*, 206 F.3d 392, 398-399 (4th Cir. 2000); *Bohach v. Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996).

[12] *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257-258 (Bankr. S.D.N.Y. 2005).

[13] *Id.* at 261.

[14] *See, e.g.*, *In re Reserve Fund Securities & Derivative Litigation*, 275 F.R.D. 154, 163-64 (S.D.N.Y. 2011); *Kaufman v. Sungard Investment Systems*, 2006 WL 1307882 at *4 (D.N.J. May 10, 2006); *In re Royce Homes, LP*, 449 B.R. 709, 737-741 (Bankr. S.D. Tex. 2011); *Alamar Ranch, LLC v. County of Boise*, 2009 U.S. Dist. LEXIS 101866, at *8-11 (D. Idaho Nov. 2, 2009).

[15] 449 B.R. at 743.

[16] *Id.* at 714, 741.

[17] We ignore the first *Asia Global* factor, which is whether the company has a policy banning personal or inappropriate communications using company devices.

[18] *See, e.g., Long v. Marubeni America Corp.*, 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) (finding that plaintiff's professed "ignoran[ce]" of the company's electronic communications policy, which allowed for company monitoring of data existing on company computers, was immaterial (and not credible), as the plaintiff "knew or should have known" about the company monitoring policy).

[19] *See e.g., Simons*, 206 F.3d at 396 ("[U]sers shall . . . [u]nderstand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate."); *Asia Global*, 322 B.R. at 260 ("The Corporation . . . reserves the right . . . to [e]ngage in random or scheduled monitoring of business communications.").

[20] *See, e.g., In re High-Tech Employee Antitrust Litig.*, 2013 WL 772668, at *7 (N.D. Cal. Feb. 28, 2013).

[21] *See, e.g., Westinghouse*, 951 F.2d at 1424-1427. It could also be argued that sharing "privileged" information with such a party might cause the privilege not to attach in the first instance. A party's expectation that a communication would be kept confidential must be "reasonable" in order for the privilege to attach. *Bingham v. Baycare Health System*, 2016 WL 3917513 at *1 (M.D. Fla. July 20, 2016).

[22] *See In re Vitamin Antitrust Litig.*, 2002 WL 35021999, at *26.

[23] *In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989); *In re Subpoenas Duces Tecum*, 738 F.2d 1367, 1373 (D.C. Cir. 1984) ("The distinction between voluntary disclosure and disclosure by subpoena is that the latter, being involuntary, lacks the self-interest which motivates the former."); *In re Vitamin Antitrust Litig.*, 2002 WL 35021999, at *28, 30-31 (finding that submissions to the Mexican Federal Competition Commission were compelled, and thus that the privilege still attached).