



E-Data Outside the Scope of U.S. Jurisdiction?
Recent Court Developments and Novel Considerations¹

Introduction:

A recent court decision provides some clarity as to when, and when not, electronic data may come within the ambit of U.S. jurisdiction. Perhaps the greatest lessons come from paying attention to when jurisdiction actually is invoked, and then working backwards to ascertain limitations on jurisdiction, which is a finite concept by definition. A situation where jurisdiction cannot be exercised over a party (lack of “personal” jurisdiction) does not mean that data owned by that party cannot be subject to a subpoena when that data is located within the United States. In *Ratliff v. Davis Polk & Wardwell*², a foreign, non-U.S. certified public accounting firm located in the Netherlands (hereinafter “CPA”), not itself subject to the U.S. Securities and Exchange Commission’s (“SEC”) personal jurisdiction, nonetheless voluntarily submitted its own audit records of its client, Baan Company, a Dutch software firm, to the SEC via its (CPA’s) counsel in the United States, Davis Polk. The SEC had launched an investigation into the CPA’s audits of Baan, which had come under earlier scrutiny for its financial reporting. In the interim and prior to this voluntary submission of data, the foreign CPA had retained the legal services of the U.S. law firm Davis Polk & Wardwell, which thereby came into custody of the CPA’s audit records of Baan, and Davis Polk submitted the records to the SEC. Baan shareholders instituted a securities fraud lawsuit against Baan in a U.S. federal court in Georgia and unsuccessfully attempted to obtain the allegedly incriminating data from the SEC, and then tried to directly subpoena same from Davis Polk & Wardwell in New York City. Davis Polk refused compliance with the subpoena, relying on *In re Sarrio*³, arguing that documentary evidence is not available from a lawyer-custodian, even absent attorney-client privilege, if the court does not have jurisdiction over CPA, the Netherlands-based client/document owner. However, on appeal the Second Circuit held that in fact the documents were subject to discovery from Davis Polk.

How could this happen? The Second Circuit held that “[D]ocuments held by an attorney in the United States on behalf of a foreign client, absent privilege, are as susceptible to subpoena as those stored in a warehouse within the district court’s jurisdiction.” The Second Circuit stated that while the documents may have been entitled to protection if they were sent to the law firm in order to obtain legal advice, once those

¹ The contents of this article are to be construed as informational only and do not replace the advice of counsel. As such, it should not be used as a substitute for consultation with professional accounting, tax, legal or other competent advisers.

² *Ratliff v. Davis Polk & Wardwell*, 354 F.3d 165 (2d Cir. Dec. 30, 2003)

³ *In re Sarrio*, 119 F.3d 143 (2d Cir. 1997)

documents were voluntarily disclosed to a third party (the SEC), any such protection ceased. More generally, a voluntary disclosure of lawyer-client communications to a third party for purposes inconsistent with maintaining confidentiality waives the attorney-client privilege as to that disclosure.⁴ The Court ruled that once documents have seen the “bright light” of public disclosure (here voluntary disclosure to the SEC), strong policy considerations favor full and complete discovery.”⁵ From this case, we can glean a substantial risk that any information brought onto U.S. shores (whether paper or electronic) may be subject to disclosure to unintended third parties, even where there is no jurisdiction over the data owner itself. Additionally, using a law firm as a document repository does not create a “wall” of protection from the jurisdictional arm of a court, and relying on assertions of “privilege” may not always create immunity.⁶

What then is the best, most practical course of action that a company can undertake to avoid the possibility of unintended data disclosure? Retaining custody of business records outside the jurisdiction of the United States, even in a situation where such records require legal examination prior to voluntary submission to U.S. agencies such as the SEC. Otherwise, there is a possibility that any records brought into the U.S., even data not disclosed to third parties, may in the final analysis become subject to subpoena and disclosure. The additional challenge is how to protect electronic data. E-data frequently is stored on backup tapes that are over-inclusive of what ultimately needs to be disclosed. The process of removing unresponsive and irrelevant data must occur outside of U.S. borders in order to prevent disclosure. This is where a non-U.S. data processing center (as is the case with nMatrix’s new London office) becomes indispensable.

Additional Risks:

There is still some risk of the disclosure of data via alternative means such as the Hague Convention (which provides in some circumstances for a litigant to petition a U.S. court for the discovery of data held abroad, but requires an actual appearance by the litigant in the foreign jurisdiction before the foreign tribunal, which normally is less

⁴ *United States v. Massachusetts Institute of Technology*, 129 F.3d 681, 684-687 (1st Cir. 1997) (government contractor's disclosure of documents to Defense Department's audit agency during agency's review of contract performance waived attorney-client privilege with regard to those documents)

⁵ *Ratliff v. Davis Polk & Wardwell*, 354 F.3d 165, 167 (2d Cir. Dec. 30, 2003)

⁶ Whether the information received from Davis Polk could also have been obtained from the SEC is not clear. We only know from the case that efforts to obtain the information from the SEC were unsuccessful.

Normally, obtaining non-public information from a government agency would require a request under the Freedom of Information Act (“FOIA”, Title 5 of the United States Code, Section 552). There are numerous exemptions which permit the SEC to avoid a FOIA disclosure. A complete listing is beyond the scope of this document, but includes data “compiled for law enforcement purposes, the release of which could reasonably be expected to interfere with law enforcement proceedings, would deprive a person of a right to a fair trial or an impartial adjudication, could reasonably be expected to constitute an unwarranted invasion of personal privacy, could reasonably be expected to disclose the identity of a confidential source, would disclose techniques, procedures, or guidelines for investigations or prosecutions, or could reasonably be expected to endanger an individual's life or physical safety.”

inclined to grant discovery).⁷ While a detailed discussion of The Hague Convention is beyond the scope of this document, in general discovery proceedings in this manner are more narrowly tailored.

A more recent development concerns private litigants in the United States attempting to utilize U.S. discovery rules to obtain disclosure of the contents of European Commission (“EC”) “Leniency Statements”. The EC, which is the European Union’s primary antitrust enforcement agency, has created incentives for companies engaging in illegal cartels to come forward (“come clean”) and thereby avail themselves of either immunity from or a reduction in fines. In the event a company does come forward to take advantage of such incentives, thereby creating a written “record” in the form of the application for leniency, that company bears the risk of treble-damage lawsuits in the U.S. for the same behavior now memorialized in the leniency application document abroad. In the *Vitamins* and *Methionine* antitrust proceedings in the U.S., attempts were made to obtain disclosure of the targeted companies’ leniency statements made in Europe.⁸ Subsequently and in response to those cases, the policy in Europe was changed to permit oral applications for leniency, thereby preventing U.S. discovery of written leniency applications. Again, this simply highlights the ever-increasing reach of the jurisdictional arm of the United States, the attempts by Europe to forestall said reach, and the need to protect corporate data from becoming unnecessarily discoverable in the first place via a properly crafted data retention and storage policy. Hence, the need for e-data processing off U.S. shores.

Additional, recent U.S. judicial precedent may lay the groundwork for troubling evidentiary fishing expeditions for discoverable materials located within U.S. jurisdictional borders to be used in unrelated foreign judicial matters – yet another reason bolstering off-shore data processing. In June 2004, the U.S. Supreme Court in *Intel Corporation v Advanced Micro Devices, Inc.*⁹ held that the provisions of Section 1782 of Title 28 of the United States Code (“28 USC § 1782”), which allows a US district court upon the application of “any interested person” to grant discovery of evidence within US jurisdictions “for use in a proceeding before a foreign or international tribunal”, does not require as a condition that the information sought be discoverable in the overseas proceeding for which discovery is requested. Therefore, there is no jurisdictional requirement that evidence sought in the United States initially be subject to discovery before the foreign tribunal in non-U.S. litigation (in this case, a matter before the European Commission). The end result is that parties may obtain evidence in the United States that is not required and/or not discoverable by a foreign court or body. The Supreme Court additionally held that § 1782 discovery may be available to complainants in the initial

⁷ See HAGUE CONFERENCE ON PRIVATE INTERNATIONAL LAW, PRACTICAL HANDBOOK ON THE OPERATION OF THE HAGUE CONVENTION OF 18 MARCH 1970 ON THE TAKING OF EVIDENCE ABROAD IN CIVIL OR COMMERCIAL MATTERS (1984)

⁸ *Re Vitamins Antitrust Litigation*, Misc. No.99-197 (D.D.C. Sept. 17, 2002) and *Re Methionine Antitrust Litigation*, Master File No.C99-3491, Report of Special Master (N.D. Cal. June 17, 2002)

⁹ *Intel Corporation v. Advanced Micro Devices, Inc.*, 542 US (2004), No.02-572

phases of overseas proceedings, and that § 1782 extends to proceedings before a broad variety of judicial and quasi-judicial entities. Even though the EC in this case submitted a brief to the U.S. Supreme Court requesting no U.S. discovery order or intervention, the Supreme Court nevertheless refused to bar discovery outright and instead remanded the case back to the District Court for further proceedings. This Supreme Court decision will result in a more liberal application of discovery rules, which does not bode well for those seeking to block discovery requests of data, both paper and electronic, situated within the United States for cases either here or abroad.

Supreme Court Justice Breyer, the lone dissenter in the aforementioned case, stressed the potential for the abuse of this legal precedent by one business competitor against another by the filing of a complaint with a European authority (e.g. antitrust) so as only to seek out information about a business rival by opening the door to liberal American discovery for use in the foreign matter. Also, Justice Breyer noted the time-consuming, high costs of discovery and discovery-related judicial proceedings. At issue were 600,000 pages of Intel documents produced during a separate lawsuit in the U.S. that Advanced Micro Devices (AMD) wanted to access as evidence against Intel in the matter before the EC. The costs of re-producing such a burdensome volume of data is staggering, not to mention time-consuming (or better put, a waste of time and resources). The moral of the story is simple: Avoid discoverability of data from the outset per a proper document retention and destruction policy, and avoid placing evidentiary materials on US soil whenever possible.

EU Directive on Data Protection and Safe Harbor:

European privacy statutes may themselves prevent certain data from leaving European soil, and again highlight Europe's more protective stance towards e-data by comparison to its American counterparts. Multinational companies need to be aware of these statutes, or else risk running afoul of these laws that have associated civil and criminal penalties. The European Union ("EU") Directive on Data Protection and Safe Harbor prohibits the transfer of personal data to non-EU countries that do not meet the European "adequacy" standard for data protection. As a result, the Directive places important burdens on U.S. and other companies that collect personal data online. While the U.S. has negotiated a "safe harbor" that permits U.S. companies to satisfy the European "adequacy" standard, substantial risks are involved where data is transferred from European to U.S. soil if said data contains personal information and is not handled appropriately per certain protocol.¹⁰

¹⁰ 1. Notice: Organizations must notify individuals about the purposes for which they collect and use personal information.
2. Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected.
3. Onward Transfer: Onward transfers (transfers to third parties) are permissible if an organization ensures the third party subscribes to the Safe Harbor principles or has other adequate safeguards in place.

In one recent example, General Motors Corporation decided to update its internal phone list. The General Motors European subsidiaries ran into the hurdle of sending personal information outside of the European Union, which would violate the abovementioned EU data privacy directive that governs how companies in Europe obtain, process and store personal information. A violation would have triggered a criminal investigation and could have resulted in fines of up to \$500,000. Ultimately the issue was resolved via use of the “safe harbor” provisions.

It is becoming evident from Leniency Statutes, European litigation, and EU privacy laws that the EU is more single-minded and conservative than the U.S. towards the dissemination of e-data beyond its borders, whether those are of a personal or business nature, as well as in the interpretation of jurisdictional reach and discovery requests.

Conclusion:

In light of these recent U.S. and European developments, now is the time for businesses and companies to strategize and revisit their paper and electronic data retention policies. Records in the possession of U.S. law firms need to be returned to clients or destroyed pursuant to a proper document retention policy. They should not be archived within U.S. law firms as a cloaking device, as this is a potential invitation to U.S. jurisdiction and discoverability. The costs alone of retaining counsel to ward off a discovery request, subpoena or jurisdictional claim can be astronomical. Companies should enter into confidentiality agreements with retained counsel prior to disclosing documents, as well as reserve the right to assert attorney-client privilege. Submitted data to U.S. counsel should be with the express directive that it is for the purpose of “legal advice”. However, that said, despite these admonishments, bells and whistles, there runs a risk that merely asserting the right to attorney-client privilege will not protect against disclosure to a third party. No “magic words” or incantations can dispel the jurisdictional reach of a U.S. court in light of recent broad interpretations of discovery rules and statutes. U.S. law firms cannot isolate their clients on their own; rather, they need to work in tandem with experienced partners to protect a clientele from inadvertent disclosure of paper and electronic data to third parties and ultimately the court system. Anticipating our customers’ needs with the opening of a European data processing office, nMatrix can apply its unparalleled expertise to work with customers to eliminate inadvertent risks of disclosure and jurisdiction, and tailor a customized solution previously unavailable in the electronic discovery industry. We invite you to contact us to discuss our services offered within the United States, Australia and our new London office.

-
4. Access: Individuals must have access to personal information about them that an organization holds and be able to correct that information where it is inaccurate.
 5. Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
 6. Data integrity: Personal information must be relevant for the purposes it is to be used for.
 7. Enforcement: To ensure compliance with Safe Harbor principles, there must be readily available and affordable independent recourse mechanisms for dispute resolution.

Source: U.S. Department of Commerce