Commentary

French Data Protection Agency Sets Parameters For Foreign Discovery of French Data

By
Steven C. Bennett

[Editor's note: Steven C. Bennett is a partner at Jones Day in New York City and Chair of the firm's E-discovery Committee. Olivier de Taffin, Ntube Sone, Gwendolynne M. Chen and Nicolas Diefenbacher assisted in the preparation of this article. The views expressed here are solely those of the Author and should not be attributed to the Author's firm or its clients. Copyright 2009 by Steven C. Bennett. Replies to this commentary are welcome.]

On August 19, 2009, the French privacy and data protection authority (the "CNIL")[1] issued an opinion (the "Opinion") addressing privacy and data security concerns that may arise under French law when U.S. litigants attempt to obtain data that falls under French jurisdiction.[2] While the Opinion does not apply to data requests from U.S. government agencies or to evidentiary issues that may surface during litigation, it may have considerable impact on U.S. litigants that seek discovery of data governed by French law.

The Opinion emphasizes the need for application of French and European data protection laws to foreign-initiated discovery requests made in France, in addition to limitations on international data transfers imposed by the Hague Convention of 1970 (the "Hague Convention"[3]). It also offers practical guidance to litigants who seek documents that fall under French jurisdiction. Litigators should note such guidance when conducting discovery of data located in France or otherwise affected by French privacy laws.[4]

Basis of Opinion: Conflict of Laws

The tension between U.S. discovery procedures and French data protection laws stems in part from the comparatively limited role that discovery plays in the French civil law system.[5] While the common law system encourages involvement of parties in collection of evidence through permissive discovery rules, civil law typically restricts disclosure of evidence to documents that are admissible at trial. More specifically, many civil law countries limit the ability of foreign litigants to reach, through discovery proceedings, data located in those countries.[6] Such limitations on foreign discovery efforts are often imposed through national laws called "blocking statutes," which seek to protect the sovereignty, as well as the economic and security interests, of the nations from which discovery is sought.[7] For example, France's blocking statute of 1968 (the "Blocking Statute")[8] prohibits foreign discovery of French data under penalty of up to six-months imprisonment, a €18,000 fine, or both.[9] This prohibition extends to anyone, regardless of citizenship or residency.

The Blocking Statute poses a significant hurdle to U.S.-originated discovery, for at least two reasons. First, the Blocking Statute may deprive litigants of documents needed to strengthen their legal positions. Second, when combined with U.S. court-mandated discovery requests, it may place the recipient of the request in a "catch 22" situation, because complying with the request may violate French data protection laws, while refusing to comply with the request may violate the U.S. Federal Rules of Civil Procedure (the "FRCP").

Nonetheless, like most jurisdictions, France allows international treaties to override the provisions of its

Blocking Statute. Specifically, the Hague Convention, to which France and the U.S. are parties, allows contracting states to request evidence under the jurisdiction of other contracting states through a Letter of Request procedure.[10]

France, however, took advantage of the Hague Convention's Article 23 (which allows signatory countries to limit the extent of their compliance with Letters of Request) by declaring that Letters of Request issued in the context of pre-trial discovery will be honored only if "the documents are specifically enumerated in the Letter of Request and have a direct and precise link with the subject matter of the litigation."[11] This requirement gives a French judge who receives a Letter of Request the discretion to decide whether to order production of documents sought under the FRCP.

Historically, attempts to circumvent the requirements of the Hague Convention were rarely criminally prosecuted in France. In 2007, however, the French Supreme Court (the Cour de Cassation) breathed new life into the Blocking Statute by upholding a fine to a France-based lawyer who tried to obtain information from a potential French witness in connection with a California litigation, without following the Hague Convention.[12] This decision suggested that overlooking the Hague Convention while conducting U.S.-based discovery in France may be problematic.[13]

Under these circumstances, and in light of increasing volumes of personal data transferred from France to the United States, the CNIL issued its recent Opinion, to address privacy concerns arising from U.S. discovery requests for data that falls under French jurisdiction.

The CNIL Opinion

In general, the Opinion reinforces the importance of the Hague Convention and French data protection laws, which stem mainly from the French Data Protection Act of January 6, 1978 or "the law on computers and liberty" (the "CL Law").[14] The CL Law regulates processing of personal data,[15] and offers various levels of protection for such data, depending on the nature of the data. In effect, the CL Law creates a three-tier framework for data processing. Sensitive data, such as data pertaining to race, ethic origin, handicap, labor union membership, and sex life, can be processed only in extremely narrow circumstances defined by the CL law. Less sensitive data, such as genetic data, criminal convictions, and other data affecting individual rights can be processed only with prior authorization from the CNIL. All other data can be processed simply by filing a declaration with the CNIL, subject to some exceptions.[16]

Violation of the CL Law is a criminal offense sanctionable by imprisonment for up to five years and fines of up to €300,000. The CL Law gives certain enforcement powers to the CNIL, including the power to reprimand violators and to publish notice of reprimand decisions; enjoin violators from continuing illegal processing; and/or impose fines.[17]

In the context of international discovery, the issue before the CNIL in rendering its Opinion was, therefore, whether the CL Law may be triggered by U.S. discovery requests, and if so, what U.S. litigants should do to comply with the law. The CNIL adopted a conservative stance regarding these questions.

The Opinion requires the person responsible for data processing (the "Data Controller") to notify the CNIL concerning any international transfers of personal data. The agency reserves the right to upgrade the declaration requirement to an authorization requirement "depending on the legal framework surrounding those data transfers." The Opinion also lays out the following guidelines for application of the CL Law in the context of discovery requests in foreign-based litigation:

1. **Responsibility of the Data Controller**. The Data Controller is the person who may direct the transfer of personal data as part of legal proceedings. This person may be connected to French territory in one of two ways: (i) by being established in France, or (ii) by conducting the data processing through technological means located in France (except where those means are used only as a conduit for the data).[18]

2. **Legitimacy of Purpose**. Data processing can take place only if the purpose is legitimate and if individual rights are protected. The person to whom the data relates (the "Data Subject") retains the ability to prevent disclosure of his or her personal information for legitimate reasons during U.S. litigation. In certain circumstances, consent of the Data Subject to disclosure of the information may be enough to

satisfy the CL Law. 19 For example, processing of sensitive personal data is generally prohibited, unless the Data Subject has consented to such processing or the processing is necessary to safeguard a legal right of the Data Controller.

3. **Proportionality**. Discovered data must be "adequate, pertinent and non-excessive" with respect to the purpose for which it is collected, which means that only information relevant to the discovery request can be transferred. Relevant information may be isolated by using filtering technologies, such as keyword searches. The proportionality and quality of the data must be objectively assessed and this operation must be done locally, i.e., in the country where the data resides. The CNIL recommends consulting a third party to assess the proportionality of the relevant data. In addition, data must be complete and accurate.

The agency notes that when personal elements, *i.e.* elements allowing identification of a person, are embedded in data and not relevant to the discovery request, the data must be made anonymous or pseudonymous before being produced. Specifically, the CNIL offers guidance on two fact patterns where the proportionality principle may be satisfied: (1) a request for production of documents made by the SEC to a French company where the personal elements of the data were not relevant to the SEC's investigation and the data was successfully made anonymous before being transferred to the SEC; and (2) a stipulated U.S. court order limited the scope of discovery by defining the boundaries of document production and laying out specific rules regarding use and access of the discovered information.

4. **Limited Duration of Storage**. Personal data can be stored only for a reasonable period, tied to the purpose of the data processing. In discovery proceedings, a reasonable period is the duration of the discovery process. The CNIL advises against using any other time frame.

5. **Discretion**. Recipients can only receive data necessary to carry out the discovery or the part of discovery they conduct.

6. **Transparency**. Data Subjects have the right to be informed in a clear and comprehensive way before data collection. When data is scheduled to be transferred outside the European Union, Data Subjects must be informed of the entity responsible for processing their data, the facts in the legal action, the link requiring disclosure of the data pertaining to the Data Subject, whether the disclosure is mandatory or optional, the consequences for the Data Subject of refusing disclosure of the data, the potential transfer outside of the European Union, and how to exercise the right to access, modify, and oppose disclosure of the information. Exceptions to the transparency principle include: (a) where informing the Data Subject jeopardizes the ability of the data collector to gather evidence, and (b) where preliminary injunctive relief ("mesures conservatoires") is necessary to prevent destruction of evidence. Under these circumstances, the Data Subject may be informed after the data transfer takes place.

7. **Right to Access and Modify**. The Data Controller must guarantee all Data Subjects the right to: (a) access data **pertaining** to them; (b) inquire as to whether the data is inaccurate, incomplete, equivocal, or expired; and (c) rectify or suppress such data. Preliminary injunctive relief may be granted to the Data Controller to maintain the confidentiality of an investigation.

8. **Security**. Access to personal data must be limited only to persons who can legitimately access the data to further the purpose(s) of the processing, *i.e.*, because processing the data is part of their job. The Data Controller must take all appropriate measures to guarantee the security of the data. In the data processing organization, the data must be separated and isolated to the extent that different departments in the organization are in charge of different aspects of processing. The CNIL also recommends that access to the data be monitored. If the Data Controller hires a service provider who can access personal data, the contract must include provisions prohibiting the service provider from using the data for any other purpose.

9. **Transfer of Personal Data to the United States**. Requirements for transfer of personal data to the United States depend on the volume and frequency of the data transferred. Small, one-time data transfers do not require authorization from the CNIL, but must be declared to the CNIL.[20] Large and/or repeat

transfers require the person or company carrying out the transfer to comply with French and E.U. privacy laws in any of the following three ways: (a) ensuring that the recipient has adequately certified compliance with the U.S. Department of Commerce's Safe Harbor Principles;[21] (b) entering into contractual provisions meeting E.U. standards for protection with the person processing the data in the U.S.; [22] or (c) adopting binding corporate rules that meet E.U. standards for protection. Finally, the CNIL suggests that U.S. jurisdictions use stipulated protective orders to limit the scope of discovery in ways consistent with E.U. data protection laws.

Conclusion

The CNIL's Opinion offers practical guidance to U.S. litigants who seek documents that fall under French jurisdiction. These guidelines may require U.S. litigants to restructure their litigation strategies or timelines to take into account the CNIL's requirements. In addition, companies that operate in France or process data that falls under French jurisdiction may need to revise their privacy policies and appoint a data protection officer, as recommended by the Opinion, to facilitate compliance with these rules. Legal counsel can offer advice and guidance on establishing or revising privacy policies and complying with French law and U.S. discovery requests.

Endnotes

1. The Commission Nationale de l'Informatique et des Libertés (CNIL) is an independent French administrative agency whose mission is to ensure that data privacy laws are properly applied to the collection, storage and use of personal data. *See* www.cnil.fr.

2. Délibération nº2009-474 du 23 juillet 2009 portant recommandation en matière de transfert de données à caractère personnel dans le cadre de procédures judiciaires américaines dites de "Discovery." [Opinion No. 2009-474 of July 23, 2009, Making Recommendations about the Transfer of Personal Data in American Discovery Proceedings.] Text available at www.cnil.fr.

3. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Oct. 7, 1972, 23 U.S.T. 2555, 847 U.N.T.S. 231 (codified at 28 U.S.C.A. § 1781 (West. Supp. 1987)).

4. Although the CNIL's authority does not extend beyond the physical limits of French territory, Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L. 281) 31, applies in the 27 countries of the European Union, plus Liechtenstein, Iceland, and Norway. Many principles from this Directive reflect the philosophy behind French privacy law, hence the influential role of CNIL opinions on the application of privacy law in other E.U. Member States.

5. As pointed out last year by the Sedona Conference, a U.S. observer of global legal trends, common law and civil law countries are in "fundamental disagreement as to how to most fairly administer justice" and this disagreement results in very different attitudes towards discovery in the two systems. The Sedona Conference, *Framework for Analysis of Cross-Border Discovery Conflicts (Public Comment Version)* at 14 (Aug. 2008).

6. *See* Steven C. Bennett & Sam Millow, *Multi-Nationals Face E-Discovery Challenges*, Int'l Fin. L. Rev. 37 (Jan. 2006).

7. *See generally* Sidney S. Rosdeitcher, *Foreign Blocking Statutes And U.S. Discovery: A Conflict of National Policies*, 16 N.Y.U. J. Int'l L. & Pol. 1061 (1983).

8. Law No. 68-678 of July 26 1968, Journal Officiel de la République Française [J.O.] [Official Gazette of France], July 27, 1968, p. 7267.

9. The Blocking Statute, art. 1 bis and 3. Article 1 bis of the Blocking Statute provides that:

   [s]ubject to international treaties or agreements and laws and regulations in force, no person shall request, try to obtain or communicate in writing, orally or under any other form, economic, commercial, industrial, financial or technical documents or information in preparation of, or as part of, foreign judicial or administrative proceedings.

10. Article 1 of the Hague Convention provides that: "In civil or commercial matters a judicial author-

ity of a Contracting State may, in accordance with the provisions of the law of that State, request the competent authority of another Contracting State, by means of a Letter of Request, to obtain evidence, or to perform some other judicial act."

11. Déclaration faite par la France le 19 janvier 1987 dans le cadre de l'article 23 de la Convention de La Haye du 18 mars 1970. [Declaration Made by France on January 19, 1987 pursuant to Article 23 of the Hague Convention of March 18, 1970.]

12. *In re Avocat "Christopher X"*, Cass. crim., Dec. 12, 2007.

13. The facts of the *Christopher X* case were not those of regular discovery requests sent to the opposing party's counsel. Christopher X had attempted to obtain the information directly from a potential witness. The inference that the prohibition in France against discovery proceedings outside the Hague Convention are not enforced may still stand in regular discovery proceedings. For a more thorough analysis of the risks involved in bypassing the Hague Convention and an enlightening summary of the treatment of the Convention by U.S. courts, please *see* Laurent Martinet & Ozan Akyurek, *The Perils of Taking Discovery to France*, The Practical Litigator, Sept. 2009, at 39-43.

14. Law 78-17 of January 6, 1978, J.O., January 7, 1978, p. 227. The CL Law was amended several times since its inception, in part to reflect the transposition of Directive 95/46/EC into French national law.

15. Like the E.U. Directive on data protection, the CL Law defines the "processing of personal data" very broadly and covers most types of information typically sought in discovery, such as e-mails, employee information, pay slips, and any information allowing identification of an individual. Mere access to data and "looking" at data constitutes "processing." CL Law art. 2.

16. Public registries open to the public and membership lists held by religious organizations are exempted from declaration. CL Law art. 8 and 22.

17. *Id.* art. 45-49.

18. Such an expansive jurisdictional scope for the Opinion is in line with the CL Law. *Id.* art. 5. It is also a natural consequence of the fundamental-rights approach to privacy, prevalent in Europe.

19. Such consent must be freely given, fully informed, and specific to the disclosed information.

20. Taken literally, Article 69-3 of the CL Law seems to allow data transfers even to a country without an adequate level of protection, as long as the transfer is "necessary… to comply with obligations aiming at acknowledging, exercising or defending a legal right." This language, which was introduced in the CL Law by amendment in 2004, is the transcription into French national law of Directive 95/46/EC's Article 26.1(d) which provides that E.U. Member States should allow transfers to countries without an adequate level of protection only if "the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims." This exception to the general prohibition against transfer to jurisdictions not ensuring an adequate level of protection could easily be construed as allowing transfers pursuant to U.S.-originated discovery requests. Yet, that is not the path followed by the CNIL, which in the Opinion allows the 69-3 exception only for "one-time, non-massive" data transfers, and even in such cases the transfer must be declared with the CNIL, although it need not be specifically authorized by the CNIL.

21. Because the United States was not recognized by France or by the European Union as providing an adequate level of data protection, the U.S. Department of Commerce, in collaboration with the E.U. Commission, has created a system of voluntary participation called "Safe Harbor" in which U.S. companies can certify their adhesion to adequate levels of protection required under E.U. law. Self-certified companies are recognized by the E.U. as offering an adequate level of protection. *See* U.S. Department of Commerce Safe Harbor webpage, www.export.gov/safeharbor.

22. According to the form contractual stipulations adopted by the European Commission, the Data Controller must conduct a thorough analysis of

the relevance, legitimacy, and accuracy of all data being transferred as part of the court proceedings. Adequate standard contractual clauses are provided in Commission Decision 2002/16, Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries, under Directive 95/46/EC, Annex, 2002 O.J. (L 6) 52, available at www.eur-lex.europa.eu. ■