Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

A Patent Litigator's Perspective On Privacy Law

Law360, New York (January 16, 2014, 12:48 AM ET) -- Patent litigations typically dredge up terabytes of data through discovery. Patent cases having nothing to do with privacy will inherently bump up against a patchwork of state, federal and international laws governing the handling of personal data. These laws occasionally surface as a major obstacle in the conduct of the case and in ancillary disputes. Following is a guide to the problems that may arise, and some best practices to avoid them, in grappling with data privacy laws in patent litigations. Of course, these issues may be germane to litigation discovery more generally.

Foreign Data

Frequently, data collection must occur from foreign sources. Your inventor may be abroad, as might a division of the company that reduced the invention to practice. You may need discovery from a prior artist abroad. Or cloud technology hosted in the U.S. may be used by customers worldwide, potentially making their data relevant to a U.S. litigation.

In any of these scenarios, and many others, foreign privacy laws govern the collection and production of the data. For European sources, the EU Data Protection Directive 95/46/EC, implemented in country-by-country laws throughout the EU, tightly restricts the use of the data in U.S. litigations without the consent of the affected individuals. Although there are exceptions for the cross-border use of EU personal data in the ordinary course of business,[1] these exceptions do not extend to the production of data in litigation. Rather, when such data is required in a U.S. litigation, absent consent, EU law provides that the data can be sought under the slow and restrictive Hague Convention.

This conflict of laws puts litigators in a bind. In a typical scenario, a party to a U.S. patent litigation who receives a document production request will object that the discovery must proceed under the Hague Convention, and move for a protective order, arguing that production under the Federal Rules will subject that party (and the lawyer) to penalties in the EU. Indeed, such penalties have been assessed.[2] However, the U.S. Supreme Court has held that foreign statutes blocking U.S. discovery "do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute."[3] Accordingly, courts in the United States will typically order the discovery to proceed.[4]

This problem is likely to get worse, not better. A new EU General Data Protection Regulation is slated to take effect in 2016 superseding the current EU directive. In addition the European Commission has proposed a new EU data protection directive that would govern the handling of personal data in criminal investigations, prosecutions and related judicial activities. It is not yet clear what impact the new regulation and directive will have on U.S. discovery obligations, but in the aftermath of the Snowden

affair and U.S. wiretapping revelations, the Europeans are likely to harden the prohibition on using EU personal data in the U.S.

Much of the world is modeled on the EU system. Latin America tends to follow Spain in its data regulations. The countries of the former British Empire tend to follow the U.K.'s lead. Korea has particularly strict laws, as well. Thus, it is important to investigate the applicable laws, and to start with the assumption that collecting data abroad will be problematic.

United States Law: State and Federal

Data privacy laws in the U.S. typically allow a judicial process exception. That is, prohibitions on data disclosures are generally subject to an exception for litigation discovery. However, it is a fact of life in litigation that things sometimes go wrong, and the judicial process exceptions may not apply. Law firms and their clients may get in trouble when a memory stick is lost, a laptop is stolen, a vendor produces the wrong data, a reviewer compromises the data, an FTP site has the wrong sharing protocols, or a computer system is hacked.

The applicable laws governing such breaches are badly splintered. Congress has been unable to enact uniform standards to govern most data privacy or data breach situations. A few exceptions are the Graham-Leach-Bliley Act (which governs how financial institutions protect personal data) and the Health Insurance Portability and Accountability Act (governing privacy of medical records). Other attempts at national standards for cybersecurity have been attempted, but ultimately unsuccessful (such as the Lieberman-Collins Act, directed to security of critical infrastructure). These federal laws establish a floor for personal data protection and do not preempt state laws that provide greater protection. State governments, by contrast, are active in promulgating data privacy laws, with 46 states having some form of privacy statutes.

California's privacy statutory framework, probably the most developed in the U.S., provides a guide to what to look for when navigating the various states' privacy laws. The California statutes most relevant to patent litigation discovery are the Financial Information Privacy Act, Confidentiality of Medical Information Act and the Security Breach Information Act. While here we focus on California privacy statutes, it is important to note that Massachusetts also has particularly strict privacy laws.

These federal and California statutes protect essentially any nonpublic personally identifiable information related to a financial transaction, or related to a patient's medical history. That includes employment information, information collected via Internet cookies or contained in a credit report, and the fact that a consumer is or has been a customer of a financial institution. The California Security Breach Act goes so far as to safeguard any nonpublic information "that identifies, relates to, describes, or is capable of being associated with, a particular individual."

"Financial institutions" may face particularly stiff fines for data breaches. The term "financial institution" is defined broadly at the federal level as "any institution the business of which is engaging in financial activities." That may encompass companies as diverse as retailers that extend consumer credit from their own accounts and businesses that lease cars, computers, or other personal or real property. This definition is narrower under California law, which excludes "any institution that is primarily engaged in providing hardware, software, or interactive services." Thus, whether a company qualifies as a financial institution will vary among different jurisdictions. Penalties for breach under California law may be as high as $2,500 for each violation "irrespective of the amount of damages suffered by the consumer as a result of that violation."

Data breaches trigger state and federal reporting requirements. Forty-six different states have their own breach reporting rules, with substantial differences among each state's requirements. For example, federal and California laws require notice to the affected individuals only for a potential breach of unencrypted personal data. Some states require notices regardless of whether the breached data was encrypted, while others, such as Minnesota, also impose a 48-hour notice period for certain types of breaches. These breach reports, which are often public, provide fodder for plaintiffs' attorneys for follow-on litigations.

Best Practices

What follows is a set of best practices derived from the language of the statutes and appropriate federal regulations, designed to reduce the risk of potentially unauthorized disclosure of personal data produced in litigation, and the associated liability for law firms and their clients.

- Segregate out personal data. This should start at the client level and continue at the law firm. Train the individuals tasked with document collection to be aware of sources of personal data. Everyone (e.g., employees, attorneys, experts, paralegals, vendors) involved in a litigation should be made aware of the privacy issues and the need to safeguard the information.

- Resist blanket calls from outside lawyers to conduct blunderbuss collections of "all documents" relating to a product, and make a thoughtful determination whether personal data needs to be collected. Consider making a disclosure to opposing counsel of the categories of personal data relevant to a lawsuit rather than producing the data. Because of the potential liabilities associated with mishandling the data, opposing counsel may accept this accommodation.

- Law firms are already accustomed to running keyword searches for privilege. Add keywords to identify personal data (e.g., "social security," "SSN," "drivers license," "passport," "routing number," "medical record"). Once identified, the personal information can be redacted (if appropriate to the case) and the documents encrypted.

- Encryption is key. Many state and federal data breach reporting laws will not apply if lost, stolen, or hacked data is encrypted. So encrypt personal data on central systems as well as when saved to travel laptops, shared on memory sticks, or produced to the other side.

- Clawback provisions for privileged documents are routinely included in protective orders. Consider expanding those clawback provisions to encompass personal information.

- Object, and if necessary move to quash, any discovery requests that seek personal data that is not directly relevant to the litigated issues. Do this early.

- Determine if data collected from U.S. companies is subject to foreign data laws (such as information about customers or ex-U.S. employees). Doing so provides additional bases for opposing foreign discovery.
- If foreign discovery is anticipated, start preparing early. Provide foreign employees with the appropriate disclosures in accordance with local laws. Whenever possible try to incorporate the consents into the engagement letter. Seek consents from the client company and relevant employees, and if appropriate from investors or other third parties at the outset of a case.

Under EU law consent must be "freely given specific and informed." When proper consent cannot be obtained, object early and aggressively seek to limit the scope of foreign discovery.

- If you anticipate the need for foreign discovery from opposing party, move early to compel discovery.

- Have a data breach notification plan. Carefully examine the notice provisions of each state where you have customers and be prepared to promptly comply with them.

- At the end of a litigation, dispose of records containing personal data in a secure manner.

—By Steven C. Carlson and Stefan R. Stoyanov, Kasowitz Benson Torres and Friedman LLP

Steven Carlson is the managing partner of Kasowitz's Silicon Valley, Calif., office. Stefan Stoyanov is an intellectual property litigation associate in the firm's New York office.

[1] See U.S.-EU & U.S.-Swiss Safe Harbor Frameworks at http://export.gov/safeharbor/ (last visited Nov. 25, 2013)

[2] In re Advocat Christopher X, Cour de Cassation, Chambre Criminelle, Paris, Dec. 12, 2007, No. 07-83228 (upholding a fine and criminal conviction against a French lawyer for collecting documents for production in a U.S. litigation.)

[3] Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. Iowa, 482 U.S. 522, 544 n. 29 (U.S. 1987) (Foreign statutes blocking U.S. discovery "do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute.").

[4] See, e.g., In re Auto. Refinishing Paint Antitrust Litig., 358 F.3d 288, 299-305 (3d Cir. 2004) (affirming lower court's order compelling foreign discovery under the Federal Rules, rather than the Hague Convention, despite contrary German laws); Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3109, 2005 U.S. Dist. LEXIS 20049, at *15-*17 (N.D. Ill. Sept. 12, 2005) (compelling an accused infringer to produce documents located in Italy pursuant to the Federal Rules despite that "Italy has explicitly stated its opposition to pre-trial discovery"); accord TruePosition, Inc. v. LM Ericsson Telephone Co., No. 11-4574, 2012 U.S. Dist. LEXIS 29294, at *22 (E.D. Pa. Mar. 6, 2012); Schindler Elevator Corp. v. Otis Elevator Co., 657 F. Supp. 2d 525, 534 (D.N.J. 2009); Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429, 456 (E.D.N.Y. 2008).