Calif. Bill On Protective Orders Threatens Privacy Norms

By **Patrick Oot and Phil Goldberg** (June 6, 2022)

Patrick Oot

Phil Goldberg

California is considering legislation that would fundamentally change the nature of civil litigation in the state in a way that threatens national and international privacy norms.

The bill — California S.B. 1149, or the Public Right to Know Act — infringes on the ability of the parties to obtain protective orders over confidential information, even when that information is subject to state, federal or international privacy laws.

The debate is largely over private documents that parties are required to share during pretrial discovery in product and environmental cases. These documents may or may not lead to admissible evidence, but parties must produce them to opposing parties that can see if any information in the documents supports their case.

When these documents contain highly confidential personal and business information, courts will issue protective orders to prevent them from becoming public.

The question is what happens to these documents after the parties resolve their dispute and the case is closed. Under current law, the documents that are subject to protective orders against public disclosure during the case largely remain so afterward.

These safeguards are critical for the ability of parties to produce materials needed in litigation, particularly when the materials are sensitive electronically stored information — from sources in California, around the country or outside the U.S.

Privacy laws, including the California Consumer Privacy Act, the federal Health Insurance Portability and Accountability Act, and the European Union's General Data Protection Regulation, restrict public disclosure of many types of information that may be contained in these documents. So, when the documents contain personally identifiable information, or PII; personal health information; or confidential business data such as trade secrets, there are penalties against their public disclosure.

Protective orders after the close of the litigation, therefore, are necessary for a litigant to comply with both the discovery orders in the case and the applicable privacy laws. In fact, a legitimized data transfer to the U.S. is only legal under the GDPR because the data is transferred for the purpose of confidential discovery and that confidential treatment governs the data the entire time it is in the U.S.

S.B. 1149 will upend this entire regime. It would make all discovery in product and environmental cases presumptively public unless the documents meet specific criteria for confidentiality — criteria that is not nearly as protective as state, federal and international privacy laws.

The bill is also one-sided; it protects PII only of a plaintiff, not of employees of the defendant companies, their customers or anyone else even if the person has no connection

to the litigation whatsoever.

The proponents of S.B. 1149 argue all of this information should be made available because it may have health or safety implications for the public. However, courts already have the authority to make documents public if doing so would have important public health or safety benefits.

Therefore, changing the law to create broad presumptions against confidentiality is not needed to protect the public, particularly when doing so will have significant privacy implications for the rest of us.

Impact on Current Efforts to Establish a U.S.-EU Data Transfer Treaty

The issue of data protection has become a huge international priority, and this legislation would directly conflict with current efforts by the Biden administration to reach agreement with the EU on a treaty governing the sharing of confidential information.

In March, the administration announced that the U.S. and the European Commission agreed to a trans-Atlantic data privacy framework and that they are trying to work out the details over the next few months.

As the administration has explained, the ability to safeguard information and data flows between the U.S. and Europe is critical for enabling the $7.1 trillion U.S.-EU economic relationship. Since 2015, the European Court of Justice has struck down two earlier attempts at reaching such an agreement, finding that U.S. safeguards on Europeans' data are not sufficient. For any EU entity to transfer data to the U.S., the data must receive the level of protection guaranteed under the GDPR.

Discovery in U.S. litigation has already been a major source of tension with GDPR compliance. U.S. discovery is much broader than civil discovery in Europe and what is allowable under the GDPR. Americans must produce material even if it has only indirect relevance to a claim, whereas the GDPR permits disclosure only of information that is relevant to or necessary for litigation. Further, what qualifies as PII is more restrictive in the EU than under California law.

Any party producing GDPR-protected data must identify any law that would hinder its ability to comply with the EU data protection law, and it cannot share the data without running the risk of significant penalties.

The GDPR penal provision states that a violation can result in a fine of up to €20 million ($21.4 million) or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever is higher. And the European Data Protection Board has affirmed that a court order does not authorize a transfer of personal data to the U.S. when doing so violates the GDPR.

As a result, litigants and courts must and regularly do enter binding agreements to manage the discovery of GDPR-protected information. These protective orders generally provide the levels of security suitable to the nature of the data and risk of disclosure. They also endure after the litigation ends, often requiring the court and litigants to destroy or return any foreign confidential information in their possession.

These protective orders are the only way to alleviate the concern that data produced in civil discovery will become public in violation of the GDPR. They must be entered before the data

is produced and last after the litigation is over.

Otherwise, the producing party cannot affirm that it can guarantee the safekeeping of the data. Because S.B. 1149 prohibits courts from providing this guarantee, parties will not be able to transfer data to California for discovery purposes if the bill is enacted.

This result would not be good for plaintiffs or defendants in cases involving GDPR-protected data, as it will make it more difficult for them to prove their case or defense.

It would not be good for the public in these cases because they will not have access to information that can be made public under existing law. And, it would not be good for the courts, as cases involving GDPR-protected data will take longer to administer, there will be more motions to address, and settlements will be harder to reach.

In the immediate term, S.B. 1149 would also throw a huge wrench into the Biden administration's efforts to reach a treaty with the EU over international data flows. As the EU's chief negotiator, European Commission President Ursula von der Leyen, said in announcing the trans-Atlantic data privacy framework, the data flows must be "predictable and trustworthy" for any treaty to be upheld by the EU high court.

Trade groups from the Computer & Communications Industry Association, which represents Silicon Valley companies, to the International Association of Privacy Professionals have been working hard to bring the sides together.

Impact on Information Americans and Europeans Hold Private

Finally, the types of cases and information at issue in these cases is vast and varied. This is not just about faceless foreign companies. Many disputes governed by the GDPR and U.S.-based privacy laws appear entirely domestic. That's because in today's global economy, much of the information Californians and other Americans hold as confidential is stored in Europe, and therefore subject to GDPR protection.

For example, a California company may outsource its information technology or human resource functions to European service providers; an American company may store information on servers located in Europe; or a California business sued in California may have a parent, affiliate, plant or subsidiary that has potentially relevant documents in Europe.

In addition, the effects on people and businesses can be harsh. For instance, S.B. 1149 purports to protect trade secrets, but only as narrowly defined in the California Civil Code. There are many other types of highly confidential commercial information, though, that do not meet this definition.

For example, say someone develops a proprietary process for compiling data on product safety trends in the U.S. and Europe. She develops an entire business based on her ability to compile and license the data to governments and other entities under strict confidentiality orders. If this information is produced in discovery and not protected, the business would lose its legal proprietary right to this information and be sanctioned by EU law for data protected by the GDPR.

Legislation similar to S.B. 1149 was introduced in Congress several years ago. The Sunshine in Litigation Act, as it was called, was widely repudiated. Groups from the American Bar Association to the federal judiciary opposed the bill.

The Judicial Conference's Committee on Rules of Practice and Procedure told the House Judiciary Committee that empirical studies show no evidence that protective orders create any significant problem in concealing information about public hazards.

The bottom line is that this legislation is not needed. Courts already have the discretion to protect the public by making important information available to them, and they can generally do so while redacting information that is protected by state, national and international privacy laws.

But the presumption that all of this information should be made public will have serious adverse consequences on the right to privacy, and given the timing, undermine the goal of critical U.S.-EU talks on data privacy.

Patrick Oot is a partner at Shook Hardy & Bacon LLP and co-chair of the firm's data and discovery strategies practice group. He is also a founder of the Electronic Discovery Institute.

Phil Goldberg is managing partner of the Washington, D.C., office at Shook Hardy and director of the Progressive Policy Institute's Center for Civil Justice.