The intersection of US litigation and EU data privacy laws

Organisations that may become involved in US litigation should consider potential obligations to retain, review and produce documents when drafting privacy policies and notices, **Laura Hall** of Allen & Overy says.

Companies with operations in the EU are increasingly finding that the broad scope of discovery in litigation in the United States is in conflict with their obligations under laws implementing the EU Data Privacy Directive. Most US courts, when considering whether production of documents in violation of foreign data privacy law should be compelled, have found that the US interest in ensuring the disclosure of all relevant information outweighs a foreign sovereign's interests in protecting privacy. The coming into force of the GDPR in May 2018, and its vastly increased potential sanctions, may cause litigants and courts to reevaluate that balance.

Document production in US civil litigation

The Federal Rules of Civil Procedure (FRCP) govern disclosure and discovery in civil proceedings in Federal courts.[1] The scope of discovery includes "any nonprivileged matter that is relevant to any party's claim or defence and proportional to the needs of the case."[2] The recipient of a request for production of documents (if a party) or a subpoena (if a non-party) must conduct a search of documents[3] in its possession, custody or control, located anywhere in the world, that is reasonable in light of the scope of discovery and where responsive information is likely to be found.[4] In a complex litigation, millions of electronic records may be collected by counsel for the parties and reviewed for privilege and responsiveness.

The recipient of a document request or subpoena may respond with objections and must state whether it is withholding any documents on the basis of those objections.[5] Most courts require the parties to meet and confer about discovery issues before they are presented to the court through a motion to compel production or a motion to quash the demand. The trial court's ruling on such a motion is generally not subject to appeal until final judgment has been reached in the case. An interlocutory appeal may be available to a party where the court orders it to produce materials contended to be subject to attorney-client privilege.

Third parties who wish to appeal an order requiring compliance with a document subpoena must disobey the order and be held in contempt of court; an appeal is then available from the contempt order, which may also impose coercive monetary sanctions (e.g. fining the party for each day it does not produce the documents). This poses a significant burden on the assertion of privileges or other objections to discovery. Parties to the litigation also may be held in contempt or otherwise sanctioned,[6] but rarely are permitted to appeal such sanctions prior to conclusion of the litigation.

> The US interest in ensuring the disclosure of all relevant information outweighs a foreign sovereign's interests in protecting privacy.

The Hague Evidence Convention

The US and 60 other countries are party to the 1970 Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention) and have thereby agreed to process requests from foreign courts for the production of documents in connection with civil litigation through their domestic legal systems. Many countries have, however, filed reservations refusing to honour requests for pre-trial disclosure of documents.

In 1987, the US Supreme Court held in *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for the Southern District of Iowa* (Aérospatiale) that ratification of the Hague Evidence Convention did not supersede the procedures for discovery provided by the FRCP with respect to foreign parties or non-parties, but rather provided "optional" procedures that could be used "whenever they will facilitate the gathering of evidence."[7] That case concerned a French "blocking statute" that makes production of evidence for foreign litigation outside the Hague Evidence Convention a crime. The *Aérospatiale* court cautioned that "American courts should … take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state,"[8] but in the vast majority of subsequent cases, little weight has been given to such interests.

Evaluating objections to production of information

The *Aérospatiale* decision did not provide "specific rules to guide this delicate task of adjudication" of domestic and sovereign interests,[9] and therefore courts have looked to the factors set out in the Restatement of Foreign Relations Law:

"In deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the United States should take into account:

(1) the importance to the investigation or litigation of the documents or other information requested;
(2) the degree of specificity of the request;
(3) whether the information originated

in the United States;
(4) the availability of alternative means of securing the information; and
(5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located."

In employing this framework, US courts nearly always conclude that compelling production under the FRCP is warranted, for several principal reasons:

First, as a result of the meet and confer prior to motion practice, the requests will have been narrowed to target information that is demonstrably relevant to a claim or defence and not available from an alternative source.

Second, in considering the "availability of alternative means," courts tend to be pessimistic about the prospects for success of a request under the Hague Evidence Convention, implicitly defining success as prompt production of all the information as would be responsive to the request under the FRCP.

Third, in balancing the interests of the United States and the foreign country, the domestic interest in full disclosure as an aid to truth-seeking in the specific case is given great weight compared to the general public interests represented by the enactment of foreign legislation. Data privacy laws are commonly mischaracterized as "blocking statutes,"[10] despite their broad domestic application, and US courts express considerable scepticism that anyone has a privacy interest in their name, address and phone number on work documents.[11] US courts also rely on exceptions, such as consent and establishment of a legal claim or defence in concluding that the transfer is in fact permitted despite experts' contentions that these exceptions do not apply or do not permit the scope of information transfer that response to a typical US document demand would require.[12] US courts also view protective orders that limit who may receive documents disclosed in the litigation as at least partially satisfying the requirements of foreign privacy laws.

Finally, US courts conclude from the absence of any reported case imposing penalties under an EU data privacy statute for disclosure in US litigation that foreign DPAs implicitly agree that the balance of interests is in favour of disclosure.

How the GDPR may change the balance

Under the GDPR, it is clear that controllers or processors who receive judgments from courts, tribunals or administrative authorities in third countries requiring them to transfer or disclose personal data cannot do so unless those requests are based on an international agreement or the GDPR conditions for transfer to third countries are met. It is likely to be difficult to satisfy the GDPR conditions in the case of transfers in connection with legal proceedings. It will require a careful assessment in each case.

In certain cases, a transfer involves the disclosure or other processing of sensitive personal data on a large scale, which may be the case where a US document demands or a subpoena would require the disclosure of information regarding possible criminal offences. In such cases, data controllers must conduct an impact assessment on an expedited basis to determine the risks of transfer and any safeguards required, and are required to notify a local supervisory authority of any resulting transfer where the identified risks cannot be effectively mitigated. A supervisory authority opinion that the transfer should not occur, or should occur in a different way, can be shared with the US court as evidence of the sovereign interests at issue in the particular case. If the US court nonetheless orders disclosure, however, notification may have increased the risk of the supervisory authority imposing a penalty.

The vastly increased penalties available under the GDPR will not alone change US courts' views about the balance of domestic and foreign interests. Based on experience to date, they are likely to expect supervisory authorities not to sanction companies that are obeying US court orders. Changing that expectation will likely require that penalties are imposed publicly in multiple cases, but there is no reason at this time to expect such penalties will be a priority of most supervisory authorities. Moreover, notwithstanding the EU-wide nature of the GDPR, its enforcement remains a local matter, and so penalties imposed by one supervisory authority may not persuade a court that a different supervisory authority is likely to follow suit.

Best practices, now and after May 2018

Data controllers who may become involved in US litigation should consider potential obligations to retain, review and produce documents when drafting privacy policies and notices. It may be possible to modify data flows so that information related to activities that may be subject to US litigation is not brought into the EU unnecessarily.

To minimize the amount of personal data transferred to the US and limit it to that truly required for the lawsuit, documents may be reviewed in the EU or another adequate country and only responsive, non-privileged documents transferred to the US. Alternatively, EU standard contractual clauses (aka model clauses) may be used with document hosting and review vendors in the US to protect information during the pre-production phase.

A company involved in US litigation should seek advice from data privacy experts on what terms should be included in the protective order and whether responses to discovery requests are likely to implicate data privacy interests so that timely objections can be interposed. In meeting and conferring over such objections, take the opportunity to educate opposing counsel about EU data privacy requirements and seek to agree on a protocol that will provide them with reasonable disclosure. For example, documents may be anonymized or pseudonymized initially and then provided de-anonymized on request for good cause (such as to authenticate a document for use at trial or to identify documents associated with a specific witness).

If an objection on the basis of data privacy law is litigated, be as specific as possible about the types of documents likely to be responsive to the document request in question, the types of personal data they are likely to contain and what information is proposed to be withheld as a consequence. If seeking to channel discovery through the Hague Evidence Convention, provide evidence that a request is likely to be successful and commit to cooperation

 © 2017 PRIVACY LAWS & BUSINESS

with foreign judicial authorities. Request support from the relevant DPA or national government in the form of an *amicus curiae* brief to the US court hearing. Such briefs have a high rate of success as they directly address the interest of the sovereign in the circumstances of the specific dispute, but some courts have ordered discovery notwithstanding the protests of foreign governments.

Conclusion

US lawyers may fail to consider the applicability of foreign law in the discovery process or struggle to explain it convincingly to a court. EU data privacy specialists may give little consideration to the realities of US litigation in designing policies and disclosures. In a world of globalized disputes and in light of the enhanced penalties the GDPR prescribes, greater awareness of the interrelation of these fields of law by practitioners of each is necessary. The price of failing to respect either may be high.

AUTHOR

Laura Hall is a Partner at Allen & Overy LLP, US.
Email: Laura.Hall@AllenOvery.com

REFERENCES

1 Most state courts' rules of procedure are modelled on the FRCP, but consideration of those rules is beyond the scope of this article.
2 FRCP 26(b)(1).
3 The term "document" in US litigation typically encompasses all forms of information storage, including audio files, electronic databases and so on, but data in relatively inaccessible form, such as disaster recovery tapes, typically need not be restored and searched.
4 Such information must be retained as soon as litigation is anticipated. See FRCP 37(e) (prescribing sanctions for loss of electronically stored information that should have been preserved).
5 FRCP 34(b)(2)(C).
6 FRCP 37 provides for fee shifting for motions to compel discovery and sanctions for failure to obey a discovery that may include directing that certain facts be considered established striking pleadings, dismissing the action and entering default judgment.
7 482 U.S. 522, 541 (1987). The regional circuit courts of appeal differ in whether they apply the *Aérospatiale* analysis at the motion to compel/quash stage or at the motion for sanctions stage.
8 *Id*. at 546.
9 *Id*.
10 See, e.g., *In re Xarelto (Rivaroxaban) Prod. Liab. Litig*., No. MDL 2592, 2016 WL 3923873 (E.D. La. July 21, 2016) (so characterizing German BDSG); *Io Grp. Inc. v. GLBT Ltd.*, No. C-10-1282 MMC DMR, 2011 WL 4974337, at *2 (N.D. Cal. Oct. 19, 2011) (UK Data Protection Act); *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *3 (C.D. Cal. May 29, 2007) (Netherlands Personal Data Protection Act); see also Statute, Black's Law Dictionary (10th ed. 2014) (defining "blocking statute" as "[a] statute prohibiting a party to request, seek, or disclose economic, commercial, industrial, financial, or technical documents or information that might lead to evidence for foreign judicial or administrative proceedings").
11 See, e.g., *Devon Robotics v. DeViedma*, No. 09-CV-3552, 2010 WL 3985877, at *5 (E.D. Pa. Oct. 8, 2010) ("Defendant only says, without citation, that email addresses may be considered personal data.") (discussing Italian data privacy law).
12 See, e.g., *In re Lernout & Hauspie Sec. Litig.*, 218 F.R.D. 348, 352-53 (D. Mass. 2003) ("In light of the self-defense exception, the court order exception and simple common sense, this Court's position is that KPMG–B must turn over copies of the audit work papers that the plaintiffs have already seen in Belgium."); *Pershing Pac. W., LLC v. MarineMax, Inc.*, No. 10-CV-1345-L DHB, 2013 WL 941617, at *9 & n.5 (S.D. Cal. Mar. 11, 2013) ("Here, disclosure can be ordered while still achieving the policies of the BDSG. MTUFN can, and allegedly has begun to, obtain consent of its employees for disclosure of documents containing the personal information."); *Devon Robotics*, 2010 WL 3985877, at *6 ("Defendant does not show why the processing of such data would not be considered an obligation imposed by (US) discovery law or why a transfer would not fall under the 'to establish a legal claim' exception.').

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Germany's new DP Act: Big news or business as usual?

The current rule of appointing a DPO in organisations remains. There is no cap on fines and there is the possibility of a criminal sentence of up to three years. By **Katharina A. Weimer,** Senior Associate, Gowling WLG, Munich.

In the midst of the "winds of change" brought by the General Data Protection Regulation (GDPR), Germany's parliament (the *Bundestag*) and the Federal Assembly (the *Bundesrat*) passed a new bill on data protection (the German Draft), waiting to be signed by the Federal President as the final step of the law-making process[1]. With the German Draft, the German government aims at implementing the

Continued on p.3

EDPS: New e-Privacy law will mean stronger enforcement

The EDPS welcomes the form of an EU Regulation for e-Privacy but calls for stronger protection for metadata, and envisages some flexibility on consent. **Laura Linkomies** reports from Brussels.

The Regulation on Privacy and Electronic Communications is proposed to take effect from 25 May 2018, and aligns with the GDPR on many aspects. In an exclusive interview with *PL&B*, Giovanni Buttarelli, the European Data Protection Supervisor, said that the GDPR will "remain incomplete without this additional exercise." He welcomes the fact that the proposal extends the scope of e-Privacy rules

Continued on p.7

Online search available
www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- Special Reports
- Materials from PL&B events
- Videos and audio recordings

See the back page or **www.privacylaws.com/subscription_info**

To check your type of subscription, contact kan.thomas@privacylaws.com or telephone +44 (0)20 8868 9200.

Issue 147 **June 2017**

PL&B Services: Publications • Conferences • Consulting • Recruitment
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

INTERNATIONAL report

ISSUE NO 147 JUNE 2017

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
K'an Thomas
kan.thomas@privacylaws.com

CONTRIBUTORS
Scott Livingston
Simone IP Services, Hong Kong

Sophie Lawrance and Noel Watson-Doig
Bristows LLP, UK

Chen Hui-ling and Michael Fahey
Winkler Partners, Taiwan

Katharina A. Weimer
Gowling WLG LLP, Germany

Laura Hall
Allen & Overy, US

Meredith Jankowski and Michelle Anderson
DLA Piper LLP, US

Chantal Bernier
Dentons LLP, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2017 Privacy Laws & Business

comment

Germany: Milestone reached in GDPR implementation

Germany has issued a new draft law to implement the provisions of the GDPR, and may be the most advanced with its plans within the EU. The draft law, adopted by the Parliament on 27 April is not easy to understand – and is in places stricter than the GDPR. For example, the law introduces the possibility of imprisonment of up to three years (p.1).

The intersection of US litigation and EU Data Privacy Laws means that controllers who may become involved in US litigation should consider potential obligations to retain, review and produce documents when drafting privacy policies and notices (p.15). The extra-territorial reach of the GDPR is a concern for non-EU companies offering goods and services in the region – when does it apply? Our correspondents analyse the situation on p.18.

An example of the global reach of the GDPR is that the US multinational Stanley Black & Decker chooses to follow the GDPR standard across its operations (p.13) in order to simplify its compliance. But companies do not have to worry about just the GDPR – plans to adopt the e-Privacy Regulation are advancing. Read on p.1 what the EDPS, Giovanni Buttarelli thinks of the proposal.

In China, new data export restrictions need companies' attention (p.9), and mean cost implications for companies as well as restrictions on their use of cloud computing. New legislative developments take place in ASEAN countries (p.25). In Taiwan, we see an increase in enforcement action (p.23).

Data protection principles come into question when determining whether a company has a dominant position under competition law, and organisations need to consider the extent to which collusion in relation to privacy policies is an area that competition authorities may investigate (p.20).

To conclude, organisations need a 'social license' to operate – the social acceptability of a business is key in the future privacy landscape, says Canada's former Interim Privacy Commissioner Chantal Bernier (p.28).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Denstu Aegis Network**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK