Walking the line: Conflicting US disclosure requirements and European privacy rules

Edward Machin and **Thomas Bannatyne** of Ropes & Gray consider the challenges faced by European businesses assessing whether to comply with US disclosure rules, particularly when doing so means potentially breaching European privacy and blocking statute requirements.

The competing interests of complying with US discovery rules and European privacy requirements existed before May 2018 and the introduction of the EU's General Data Protection Regulation ("GDPR"). Indeed, organisations that are party to litigation in American courts or subject to US regulatory investigations have long faced a choice: comply with the demands of document discovery and risk penalties in Europe, or resist disclosure and incur the wrath of an American judge or regulator.

France exemplifies this tension. The French Blocking Statute has been in force since 1968 and prohibits the request, search for or disclosure of French commercial information for use in foreign judicial proceedings. Though a national security measure rather than a privacy-specific requirement, the Blocking Statute shows the problems of conflicting legal obligations across borders. It arises in part from a clash of legal cultures: French law requires the disclosure only of evidence that a party will rely on it to make its case, whereas US discovery has a sweeping reach that can cover persons other than the parties to litigation holding relevant documents. So what are European organisations to do when faced with a US discovery order or regulatory request?

Historically, low levels of enforcement have made the choice simple. The consequences of non-compliance with an order from US courts or regulators are both more severe and more likely to follow from a refusal to co-operate than enforcement by a European regulator. That broadly remains the case, notwithstanding a small number of recent actions that have focused minds on this side of the pond (see, for example, decision 6B_216/2020 of the Swiss Federal Supreme Court in November 2021 to convict an asset manager who had transferred client data to the US in the context of a tax dispute). Many American companies also view their regulatory obligations through the prism of US law, such that European concerns are often given lesser weight.

Enter the GDPR?

A heightened global focus on data protection in general, and on trans-Atlantic data transfers specifically following the European Court of Justice's decision in *Schrems II*, is increasing the pressure on European organisations to consider how to handle US discovery requests. But if the calculations have changed, the conclusion seems largely to be the same – at least for now. The wrath of US courts and regulators continue to weigh the scale towards forcing discovery, particularly where good will in a judicial context resulting from cooperation requires the organisation to fully open its books. As such, and despite their possible reservations, parties are usually willing to step out onto the tightrope.

> The ICO's business-friendly interpretation of GDPR derogations may mean that Art. 49(1)(e) can also be used as a helpful solution in addressing at least some concerns that companies have.

Though not necessarily explicit in the publicised American judgments, there is perhaps a sense that European privacy concerns are being used as a litigation strategy. A common theme is that parties cannot hide behind foreign privacy laws to circumvent discovery rules, and this may reflect the view that arguments from those exposed to penalties from European regulators are motivated neither by genuine privacy concerns nor worries about the financial and reputational consequences of enforcement. The tone was set by the pre-GDPR case of Aerospatiale[1], and the tendency towards ignoring European privacy concerns in US litigation continues to be strong.

Aerospatiale and the cases that followed set out a five-factor balancing test with which to weigh the competing interests of US courts and European privacy laws. In brief, these cover :

(1) the importance of the data in question to the litigation,
(2) the degree of specificity of the disclosure request,
(3) whether the data originated in the US,
(4) the availability of alternative means of securing the information, and
(5) the extent to which non-compliance undermines important interests of the US versus whether compliance undermines important interests of the relevant foreign state.

Applying this test, if the data are important to the litigation, and are the subject of a specific request originating in the US or are otherwise unavailable to the court, the case law suggests that the American judiciary will tend towards requiring disclosure by the party relying on the foreign privacy law.

A history of non-enforcement by European courts and regulators

appears to make the fifth *Aerospatiale* limb close to a foregone conclusion for US judges. For example, this reticence to weigh into what is partially a geopolitical issue perhaps supports the view of these judges that blocking statutes and the GDPR do not represent important interests of the relevant European states. If they did, the thinking goes, they would be regularly enforcing their laws. With limited risk of serious consequences for breaches of European law (at least to date), the potential damage to the interests of the party resisting disclosure is, for many organisations, a risk worth taking. In order to turn this limb of the test to their advantage, the party resisting disclosure must not only demonstrate that the GDPR (or another foreign law) applies, but also that the consequences of a breach justify undermining the interests of US litigation.

Whilst the record of national regulators makes the second point difficult to establish, case law suggests that parties themselves often struggle to establish the first. In *Woldegiorgis*[2], the argument that the GDPR – as well as Philippine data protection law – precluded production of personal data was not found to be persuasive. Likewise in *Rollins Ranches*[3], the defendant was unable to convince the court that the UK Data Protection Act and the GDPR applied, and in *Vesuvius*[4] a decisive factor was that the party resisting disclosure could not establish that any enforcement action from a European data protection authority would follow disclosure.

A PATH FORWARD?

What then can businesses do to address European privacy concerns arising during discovery and regulatory enquiries – even if those concerns appear not to be a current focus for regulators in the EU? In some cases, privacy concerns seem to fall away because the US court is not convinced that discovery and privacy laws are incompatible at all. Stronger arguments on this point may start to reverse the trends in these decisions and force American judges to give other elements of the balancing test more weight. For example, if discovery can be shown to be non-compliant with the GDPR, the implicit presumption in favour of US litigation and regulatory processes may at least be weakened. Parties seeking to resist disclosure would no doubt welcome a test case or regulatory action in Europe establishing clear incompatibility between US disclosure practices and European data privacy laws – if for no other reason than to help quantify the risks that businesses face in acquiescing to the demands of US courts or regulators when producing documents containing personal data.

In some limited circumstances it may be possible to sidestep the issue. A difference of opinion – albeit small, but potentially useful – between the UK and the EU in relation to the use of derogations to the GDPR's transfer requirements could help to assuage businesses in the UK that they can comply with both GDPR and US regulatory disclosure rules. In January 2021, the UK Information Commissioner's Office ("ICO") stated that, in the context of personal data transfers to the US Securities and Exchange Commission ("SEC"), the public interest derogation (Art. 49(1)(d)) of the GDPR can be relied on to transfer data in order to meet the requirements of the SEC's books and records rule (*PL&B UK* March 2021, p.4). The extent to which the GDPR's transfer derogations apply more broadly to disclosure in litigation or regulatory requirements remain untested, but the ICO's business-friendly interpretation of GDPR derogations may mean that Art. 49(1)(e) – i.e., the establishment, exercise or defence of legal claims – can also be used as a helpful solution in addressing at least some concerns that companies have when sending data to the US for litigation and investigatory purposes.

Where genuine privacy concerns exist, mitigation is also available – at least in part. In both *Vesuvius* and *SEC v Telegram*[5], redaction was permitted to enable the production of documents for the purposes of litigation. In *AnywhereCommerce*[6], a protective order that designated certain documents as "for attorneys' eyes only" afforded European data subjects greater protection than other documents which were disclosed. For that reason, it is important for European entities facing US litigation or regulatory probes to identify, at an early a stage as possible, where cross-border discovery or data transfers may be required. This will help them to consider measures to protect data shared internationally (for example, by protective order, redaction or confidentiality agreements) and to reduce the volume of the data that are produced.

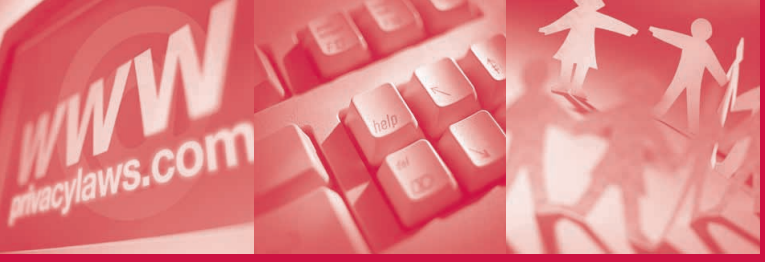
Recent case law makes clear that US courts will not routinely waive discovery requirements to accommodate foreign businesses' privacy obligations, even where they are persuaded that the GDPR does properly apply. For that reason, businesses walking the tightrope must perform their own assessment – both to determine the various costs of defying the requirements of the US courts and the risks involved in transferring data without fully complying with the GDPR or violating the requirements of a national blocking statute. This assessment will inevitably evolve as the regulation of trans-Atlantic data flows develop. But whatever shape this regulation may take, tension between the interests of European data subjects, the legal requirements to which European businesses are subject, and US courts and regulators is likely to remain.

AUTHORS

Edward Machin is an Associate at Ropes & Gray LLP in London. Thomas Bannatyne is a Trainee Solicitor at the same firm.
Emails: Edward.Machin@ropesgray.com
Thomas.Bannatyne@ropesgray.com

REFERENCES

1 Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa [1987]
2 Woldegiorgis v NYK Ship Management [2021]
3 Rollins Ranches LLC et al. v Watson [2020]
4 Vesuvius USA Corp. v Phillips [2020]
5 SEC v Telegram [2020]
6 Anywhere Commerce Inc. v Ingenico Inc. [2019]



ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

DPO conflicts – navigating the minefield with care

Whether your DPO is full-time in-house, external or also fulfils other roles, the appointee will have to find a way to navigate through a myriad of potential conflict of interest situations. By **Alison Deighton** and **Samantha Jaggers** of HelloDPO Ltd.

Some DPOs are dedicated full time to their role but may be appointed as the DPO for a group of companies. What happens when one group company acts as processor for other group companies? Does that create a conflict of interest for the DPO? Some DPOs have other roles to fulfil. If your DPO is also your head of legal, what happens

Continued on p.3

Consents, records and disguises: Lessons from ICO direct marketing enforcement

Rebecca Cousin, **Cindy Knott** and **Alex Buchanan** of Slaughter and May explain what organisations should be aware of.

The past year has seen a continued trend of enforcement action by the Information Commissioner's Office (ICO) for breaches of the direct marketing rules contained in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Whilst a number of these actions are directed at persistent unscrupulous

Continued on p.5

Issue 121 **MAY 2022**

UNITED KINGDOM
report

ISSUE NO 121 **MAY 2022**

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Alison Deighton and Samantha Jaggers
HelloDPO Ltd
Rebecca Cousin, Cindy Knott and Alex Buchanan
Slaughter and May
Gareth Oldale and Harriette Blake
TLT LLP
Edward Machin and Thomas Bannatyne
Ropes & Gray LLP
Katie Hewson, Olivia Fraser and Jonathan Howie
Stephenson Harwood LLP

PUBLISHED BY
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Email: info@privacylaws.com
Website: www.privacylaws.com

Subscriptions: The *Privacy Laws & Business* United Kingdom 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 2047-1479

comment

Information Commissioner keen to bring certainty

As the new Information Commissioner, John Edwards, has recognised, UK DPOs have had a heavy workload in the last few years with the introduction of the GDPR, implications of Brexit and now some uncertainty over the UK's future data protection framework. While we expect to see more concrete proposals from the DCMS any day now, the Commissioner reassures companies that he wants stability (p.18).

Edwards seems willing to be a strong enforcer. He now has some old cases to see through – for example the Experian appeal at the First Tier Tribunal (p.13).

The government has proposed some changes to the ICO's enforcement powers; firstly the ICO would be able to commission an independent technical report to inform its investigations into an organisation's activities. Secondly, Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR) fines would go up to GDPR levels. Given the ICO's previous focus in this area, this could be significant for companies (p.1).

Edwards is keen to cooperate with his EU counterparts but at the same time sees some benefit of being outside of the EU. In an interview with *Politico*, he said that 'What we have at the ICO as our competitive advantage, I think, is an ability to move fast and fix things and not be mired down by the bureaucracy of needing to check with 20 colleagues on every bit of wording on every penalty.'

DPOs must be experts in data protection, but also independent and adequately resourced, and report to the highest management level. However, in some situations conflicts may arise (p.1).

The government proposed to scrap the mandatory DPO role. It remains to be seen whether this unpopular idea has now been abandoned. Join us on 25 May to hear the latest from the DCMS and give your views in a roundtable in London. We also welcome you once again to join in our wonderful summer school atmosphere at St John's College, Cambridge, for a three-day information-packed *PL&B* Annual Conference 4-6 July (worth 12 CPE credits). See www.privacylaws.com/plb2022 for details.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO plans.

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

Be alert to privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
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.

3. Electronic Versions
We will email you the PDF edition which you can also access in online format via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

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

privacylaws.com/reports

"*Privacy Laws & Business* not only acts as a useful and comprehensive summary of recent key developments in our area of specialism, but also provides excellent, in-depth insight and analysis to drive thought leadership. It's an invaluable source of information."

Emma Erskine-Fox, Managing Associate, TLT LLP

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 36th year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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