The prospects for FTC Privacy Rules: Still a long road ahead

Andrew Smith and **Yaron Dori** of Covington discuss the Federal Trade Commission's ambitious plans to regulate in the field of commercial data privacy.

In August of this year, the Federal Trade Commission (FTC) released an Advance Notice of Proposed Rulemaking (ANPRM or Privacy ANPRM) to seek public comment on "commercial surveillance" practices that potentially harm consumers.[1] Specifically, the Privacy ANPRM broadly asks whether the agency "should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies (1) collect, aggregate, protect, use, analyze, and retain consumer data, as well as (2) transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive." More than 11,000 comments on the Privacy ANPRM were received before the public comment period ended on 21 November.[2]

The FTC appears to have set an ambitious agenda for itself – devising a rule to govern data collection, use and transfer throughout the entire economy, while also regulating automated decision-making, algorithmic discrimination, data about children and teens, and a host of other objectives. As described below, this already ambitious task will be made harder by an ANPRM that is very wide ranging and does not put stakeholders on notice of the alternatives under consideration, as required by statute; a federal judiciary that increasingly is sensitive to overreach by administrative agencies; challenges demonstrating that specific practices are unfair and otherwise harmful to consumers; and a lack of concrete, defined, and coherent goals for the rulemaking effort.

Background

The Privacy ANPRM itself was not unexpected. The FTC indicated earlier this year in a submission to the Office of Management and Budget that it was considering initiating a "Trade Regulation Rule" proceeding to "curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."[3] And, last year President Biden issued an Executive Order "encouraging" the new Chair of the FTC, at her discretion, to make rules regulating "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[4]

While the Privacy ANPRM described the potential subject matter of the regulation, it provided little or no detail on the objectives that the FTC is seeking to achieve or the various regulatory alternatives under consideration.

It is possible that new rules are not even the goal of the Privacy ANPRM. The ANPRM acknowledges that if new rules are not forthcoming, the record developed in response to the ANPRM nevertheless will "help to sharpen the Commission's enforcement work and may inform reform by Congress or other policymakers."

Notably, if the Commission were to successfully promulgate one or more new data privacy rules, anyone who violates a rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule" could be liable for civil penalties of more than $40,000 for each violation.[5]

FTC authority to make "Trade Regulation Rules"

The FTC has authority to issue economy-wide "Trade Regulation Rules" prohibiting unfair and deceptive trade practices.[6] Because of the breadth of this authority, the procedural requirements imposed on the FTC to make a Trade Regulation Rule are significantly more stringent than what is required under the Administrative Procedure Act for notice-and-comment rulemaking.[7]

First, the agency must provide an Advance Notice Of Proposed Rulemaking to Congress describing the area of inquiry, the objectives to be achieved by rulemaking, and potential regulatory alternatives.[8] This is all the FTC has done thus far. The FTC then must publish for public comment a Notice of Proposed Rulemaking (NPRM) that describes with particularity the reasons for the proposed rule and potential alternatives, with a cost-benefit analysis for each.[9]

The NPRM must include "disputed issues of material fact" designated by the Commission to be "material and necessary to resolve," and an opportunity for an informal hearing, if an interested person requests to present their position orally. A request to add disputed issues of material fact beyond those identified in the NPRM may be made in the hearing request. If a hearing has been requested, the FTC then must publish a Notice of Informal Hearing. Interested parties are entitled to present evidence and, if necessary, cross examine witnesses with respect to disputed issues of material fact.[10] Following the hearing, the Presiding Officer makes a recommended decision with a proposed resolution of disputed issues of material fact.

The FTC then reviews the recommendation and rulemaking record and may take additional testimony before promulgating a Final Rule.

Does the ANPRM Comply with the Statutory Requirements?

Under the FTC Act and the agency's Rules of Practice, an ANPRM for a Trade Regulation Rule must contain "a brief description of the area of inquiry under consideration, the objectives which the Commission seeks to achieve, and possible regulatory alternatives under consideration by the Commission."[11] Although the Privacy ANPRM briefly describes the area of inquiry, it does so only in the broadest of terms – focusing, for example, on all collection, use, disclosure, and security

of personal data, employee data and business data; personalized advertising; automated decision-making; algorithmic discrimination; consumer notice; and whether there are unique harms for children and teenagers – and it does not describe the objectives which the FTC seeks to achieve, the regulatory alternatives under consideration by the FTC, or even the harm that such a rule would seek to prevent.

Indeed, the ANPRM appears to concede this point, effectively stating that it is "too soon to tell" the regulatory approach that the FTC might take: "The Commission is wary of committing now, even preliminarily, to any regulatory approach without public comment given the reported scope of commercial surveillance practices."[12] Given the breadth of the ANPRM, as well as the limited evidence it presents regarding the practices that harm consumers, it seems possible that the record will support conclusions by the agency about whether to regulate, how best to regulate, the various options for regulation, or even why it is considering regulation. Also of concern is that the ANPRM is required to put stakeholders on notice of the potential requirements or prohibitions that the FTC may impose, to allow them to marshal evidence regarding the costs and benefits of those regulatory options. The ANPRM does not appear to meet this standard, either.

The rulemaking could be based on the FTC's enforcement record

To justify a Trade Regulation Rule, the FTC must state with particularity the unfair or deceptive acts or practices which are the subject of the proposed rulemaking and the manner and context in which such acts or practices are unfair and/or deceptive. The FTC also must demonstrate that these acts or practices are "prevalent" based on prior FTC's cease-and-desist orders or "other information" indicating a "widespread pattern of unfair or deceptive acts or practices."[13]

Most FTC privacy and data security enforcement actions have alleged that the defendant engaged in deception – defined as a practice that is likely to mislead consumers acting reasonably under the circumstances to their detriment.[14] Examples include allegedly misleading disclosures in a company's privacy policy regarding how the company collects, uses, transfers, or safeguards personal data.[15] Because these types of harms are typically remedied either by refraining from the misleading statement, or providing an adequate disclaimer to set the record straight, substantive requirements or prohibitions, such as requiring companies to provide consumers with access to data about them and an opportunity to correct or delete those data, as some state laws now require,[16] they would need to be premised on the FTC's authority to prohibit "unfair" practices. Indeed, last year's Executive Order called for the FTC to make rules regulating "*unfair* data collection and surveillance practices," making no mention of deception.[17]

Under the FTC Act, a practice is unfair only if: (1) it "causes or is likely to cause substantial injury to consumers;" (2) the injury "is not reasonably avoidable by consumers themselves;" and (3) the injury is "not outweighed by countervailing benefits to consumers or to competition.[18] Moreover, a "substantial injury" usually involves a monetary harm, and emotional impact and other more subjective types of harm will not render a practice unfair.[19]

The ANPRM lists dozens of FTC enforcement actions, ostensibly intended to demonstrate the need for privacy and data security rules and the prevalence of certain harmful practices.[20] There are several enforcement actions cited in the ANPRM that allege unfair privacy or data security practices, but they fall into a limited number of categories:

- companies that allegedly sell sensitive data (such as financial data or phone data) to potential fraudsters and/or contrary to clearly expressed expectations of consumers;[21]
- companies that allegedly post sensitive personal information, including financial, healthcare, or intimate information (i.e., "revenge porn"), on the Internet, and do not allow consumers to request its removal;[22]
- companies that allegedly install – or allow others to install (i.e. "stalkerware") – software on consumer devices that creates security vulnerabilities or secretly transmits personal and intimate data to third parties;[23]
- companies that allegedly fail to implement basic, readily available, low-cost, and well-known data safeguards;[24]
- companies that allegedly track consumers' television viewing behavior without their knowledge or consent;[25] and
- companies that allegedly make material changes to their privacy policies without affirmative consent for data already collected under the prior policy.[26]

Some of these areas of inquiry – such as "stalkerware," "revenge porn," sale of bank account data to fraudsters, or failure to adopt obvious and well-known data security safeguards – could conceivably support an unfairness rulemaking. Indeed, an ANPRM focused on these practices would be based on the agency's actual enforcement experience, appropriately tailored to allow for meaningful public comment, and provide the FTC with a more manageable rulemaking task. But the ANPRM casts a much wider net.

Major questions doctrine

Compounding the FTC's difficulty with showing that specific privacy practices are "unfair" is an increasing tendency by federal courts to not defer to agency determinations where the agency is using a broad grant of authority to regulate an area not specifically contemplated by Congress. An example of this is the "major questions doctrine," under which the Supreme Court has rejected agency claims of regulatory authority when the underlying claim of authority concerns an issue of "vast 'economic and political significance'" and Congress has not clearly empowered the agency with authority over the issue.[27] In its most recent term, *the Supreme Court, in West Virginia v. EPA,*[28] explicitly referred to the major questions doctrine to invalidate agency action, holding that Congress "conspicuously and repeatedly declined to enact" a program similar to aspects of the challenged regulation.

The FTC's privacy rulemaking could raise this same concern – based

on a very general grant of authority to make rules prohibiting "unfair or deceptive" trade practices, the FTC now is contemplating a broad rule regulating every aspect of data collection, use and transfer throughout the economy. And, data privacy and security is an area where Congress has explicitly declined to act in recent years,[29] exacerbating the question of whether Congress specifically authorized the FTC to make rules where Congress had declined to do so.

Conclusion

The FTC's ANPRM is ambitious. But given the statutory requirements to which FTC rulemaking is subject, this ambition may prevent it from realizing its objectives. If shining a spotlight on data privacy practices is at the core of the FTC's objective, then the ANPRM and the attention it generates may well be effective. But if its goal is to promulgate durable data privacy rules that will withstand judicial scrutiny, then the outcome is likely to be far less certain.

AUTHORS

Andrew Smith is a Partner at Covington in the US, and was previously Director of the Bureau of Consumer Protection at the FTC.
Yaron Dori is a Partner at Covington in the US.
Emails: asmith@cov.com
ydori@cov.com

REFERENCES

1 87 Fed. Reg. 51,273 (August 22, 2022).
2 This article updates an earlier article on the same topic, entitled "Prospects for FTC Privacy Rules." See *PL&B International Report*, August 2021, p.15
3 The FTC is authorized under Section 18 of the FTC Act, 15 U.S.C. § 57a, to make broad, economy-wide, "Trade Regulation Rules" prohibiting practices that it has reason to believe are "unfair" or "deceptive."
4 See White House, *Executive Order on Promoting Competition in the American Economy* (July 9, 2021), www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/.
5 See 15 U.S.C. Sec. 45(m)(1)(A).
6 15 U.S.C. § 57a.
7 See 5 U.S.C. § 553(b)–(e) (2012) (prescribing the procedural requirements of notice-and-comment rulemaking).
8 See 16 CFR § 1.10.
9 See id at § 18(b)(3)(B).
10 See 16 CFR § 1.10.
11 15 U.S.C. § 57a(b)(2)(A)(i); 16 CFR § 1.10(b)(1).
12 87 Fed. Reg. at 51,281, note 127.
13 See 16 CFR § 1.14(a)(1).
14 See FTC Policy Statement on Deception (Oct. 14, 1983), appended to In re Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf
15 See Federal Trade Commission, *FTC's Use of Its Authorities to Protect Consumer Privacy and Security* (2020), www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf.
16 See California Privacy Rights Act, § 1798.105(a) & §1798.106(a) (2020); Virginia Consumer Data Protection Act, § 59.1-573(A)(2)&(3) (2021); Colorado Privacy Act § 6-1-1304 (1)(b)&(c) (2021).
17 See White House, *Executive Order on Promoting Competition in the American Economy* (July 9, 2021), www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/ (Emphasis added.)
18 15 U.S.C. § 45(n).
19 Federal Trade Commission, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness
20 87 Fed. Reg. at 51,278-79.
21 Compl. for Permanent Injunction and Other Equitable Relief, FTC v. Blue Global & Christopher Kay, 2:17-cv-02117 (D. Ariz. filed July 3, 2017), www.ftc.gov/system/files/documents/cases/ftc_v_blue_global_de01.pdf; Compl. for Permanent Injunction and Other Equitable Relief, FTC v. Sequoia One, LLC, Case No. 2:15cv-01512 (D. Nev. filed Aug. 7, 2015), www.ftc.gov/system/files/documents/cases/150812sequoiaonecmpt.pdf; Compl. for Permanent Injunction and Other Equitable Relief, FTC v. Sitesearch Corp., No. CV-14-02750-PHX-NVW (D. Ariz. filed Dec. 22, 2014), www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf; Compl. for Injunctive and Other Equitable Relief, United States v. Accusearch, Inc., No. 06-cv-105 (D. Wyo. filed May 1, 2006), www.ftc.gov/sites/default/files/documents/cases/2006/05/060501accusearchcomplaint.pdf
22 Compl. for Permanent Injunction and Other Equitable Relief, FTC and State of Nevada v. EMP Media, Inc., No. 2:18-cv-00035 (D. Nev. filed Jan. 9, 2018), www.ftc.gov/system/files/documents/cases/1623052_myex_complaint_1-9-18.pdf; Compl., In re Craig Brittain, F.T.C. File No. 132-3120 (Dec. 28, 2015), www.ftc.gov/system/files/documents/cases/160108craigbrittaincmpt.pdf; Compl., United States v. Mortg. Sols. FCS, Inc., No. 4:20-cv-00110 (N.D. Cal. filed Jan. 6, 2020), www.ftc.gov/system/files/documents/cases/mortgage_solutions_complaint.pdf
23 Compl., In re Support King, LLC, F.T.C. File No. 192-3003 (Dec. 20, 2021), www.ftc.gov/system/files/documents/cases/1923003c4756spyfonecomplaint_0.pdf; Compl., In re Retina-X Studios, LLC, F.T.C. File No. 172-3118 (Mar. 26, 2020), www.ftc.gov/system/files/documents/cases/172_3118_retina-x_studios_complaint_0.pdf; Compl. for Permanent Injunction and Other Equitable Relief, FTC v. CyberSpy Software, LLC., No. 6:08-cv-01872 (M.D. Fla. filed Nov. 5, 2008), www.ftc.gov/sites/default/files/documents/cases/2008/11/081105cyberspycmplt.pdf; Compl., In re DesignerWare, LLC, F.T.C. File No. 112-3151 (Apr. 11, 2013), www.ftc.gov/sites/default/files/documents/cases/2013/04/130415designerwarecmpt.pdf; Compl., In re Aaron's, Inc., F.T.C. File No. 122-3264 (Mar. 10, 2014), www.ftc.gov/system/files/documents/cases/140311aaronscmpt.pdf; Compl. for Permanent Injunction and Other Equitable Relief, FTC v. FrostWire LLC, No. 1:11-cv-23643 (S.D. Fla. filed Oct. 7, 2011), www.ftc.gov/sites/default/files/documents/cases/2011/10/111011frostwirecmpt.pdf
24 Compl., In re Residual Pumpkin Entity, LLC, F.T.C. File No. 1923209 (June 23, 2022), www.ftc.gov/system/files/ftc_gov/pdf/1923209CafePressComplaint.pdf. We note that the vast majority of data security cases have been premised not on unfairness but on deception.
25 Compl. for Permanent Injunction and Other Equitable and Monetary Relief, FTC v. Vizio, Inc., No. 2:17cv-00758

REFERENCES

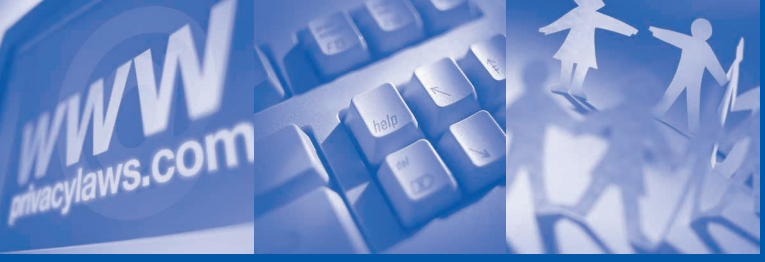
(D.N.J. filed Feb 6, 2017), www.ftc.gov/system/files/documents/cases/170206_vizio_2017.02.06_complaint.pdf. We note that this could perhaps have been pleaded as a deception claim, and any consumer harm would be remedied with a clear disclosure or consumer notice and consent.

26 In re Gateway Learning Corp., F.T.C. File No. 042-3047 (Sept. 10, 2004), www.ftc.gov/sites/default/files/documents/cases/2004/09/040917comp0423047.pdf.

27 Util. Air Regul. Grp. (UARG) v. EPA, 573 U.S. 302, 324 (2014) (citing FDA v. Brown & Williamson Tobacco Corp., 529 U. S. 120, at 159 (2000)).

28 142 S. Ct. 2587 (2022) on carbon dioxide emissions from existing coal- and natural-gas-fired power plants

29 *Washington Post* Editorial Board, "Enough failures. We need a federal privacy law." (March 30, 2022) ("After repeated failures, Congress is reportedly attempting again to forge a federal privacy law.").



ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

An update on compensation claims under the EU GDPR

CJEU Advocate General: No compensation for mere upset feelings. By **Lore Leitner**, **Arjun Dhar**, **Josephine Jay** and **Miles Lynn** of Goodwin.

The EU General Data Protection Regulation (GDPR), under Art. 82, provides the right for any person who has suffered material or non-material damage as a result of a GDPR infringement to receive compensation. However, what constitutes "non-material damage" and the associated level of damages to be awarded has long been a contentious topic in European jurisprudence.

Continued on p.3

Latin America's EU linked Model Contractual Clauses for international data transfers

A session at the Global Privacy Assembly explained how Model Contract Clauses are creating business value in Latin America. **Stewart Dresner** reports from Istanbul.

Standard and Model Contractual Clauses, as a legal basis for transferring personal data between jurisdictions, create business value while protecting individual rights, and have advantages over consent (which can be withdrawn) and Binding Corporate Rules (usually

Continued on p.5

Issue 180 **DECEMBER 2022**

INTERNATIONAL report

ISSUE NO 180 DECEMBER 2022

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@privacylaws.com

CONTRIBUTORS
Lore Leitner, Arjun Dhar, Josephine Jay and Miles Lynn
Goodwin, UK
Andrew Smith and Yaron Dori
Covington, US
Katharina A. Weimer and Carolin Wagner
Fieldfisher, Germany
Andin Aditya Rahman
Indonesia
Edward Taelman, David van Boven and Marie Barani
Allen & Overy LLP, Belgium
Masao Horibe
Hitotsubashi University, Japan

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* 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

comment

If you can take your eye off the ball, watch the app!

The World Cup in Qatar has attracted attention to many aspects other than football itself, one of them being lack of privacy. The tens of thousands of surveillance cameras using facial recognition technology prompted France's DPA, the CNIL, to advise football fans to use a burner mobile (an inexpensive prepaid anonymous phone) in order to safeguard their personal data. Germany's federal DPA has also issued a warning about Qatar's data collection via World Cup apps and advised visitors to not take their usual phone to Qatar due to excessive data collection via the app. Ironically, Qatar has had a data protection law in force since 2017, but is not on the list of jurisdictions regarded by the EU as "adequate".

The dilemmas posed by facial recognition technologies was one of the issues debated by the DPAs at their annual international conference in Turkey, where they adopted a resolution on this technology (p.21). Stewart Dresner and I attended the open days of the conference. Read an overview of the proceedings on p.17 and the latest news about Latin American Standard Contractual Clauses and other developments in the region on p.1.

Indonesia's data protection law in now in force – a major change in the world's fourth-most populous country (p.22). Bangladesh has prepared a Bill (p.26) and the EU has several Acts in the pipeline that will affect the data protection framework. The draft AI Act is making progress, and the Digital Services Act, EU's new online content regulation, has been in force since 16 November. Companies now have until 17 February 2024 to ensure compliance (p.27).

In the US, a debate has started about the Federal Trade Commission's rulemaking in the fields of consumer privacy and data security (p.8). The FTC's focus is very much on behavioural advertising. Some commentators are however questioning the FTC's authority to engage in privacy rulemaking, especially now as there are attempts in the US Congress to adopt a federal level privacy law.

Our Germany correspondents report on data transfers in the context of US-based subsidiaries, and the application of *Schrems II* (p.12). We also bring you an analysis of a recent Advocate General's Opinion from the Court of Justice of the European Union on compensation under the EU GDPR (p.1).

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

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 168+ countries alongside legal analysis, management guidance and corporate case studies.

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

Stay informed of data protection legislative developments in 168+ 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 administrative 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 and 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 Version**
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 and related laws.

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

7. Events Documentation
Access 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

> *PL&B International Report* is a very useful and business-friendly publication that allows our team to easily and frequently keep up with developments in countries outside our jurisdictions of activity.
>
> **Magda Cocco and Inês Antas de Barros, Partners and Isabel Ornelas, Managing Associate, Information, Communication & Technology Practice, Vieira de Almeida, Lisbon**

UK Report

Privacy Laws & Business also publishes *PL&B UK Report* six times a year, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

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.