GDR

THE GUIDE TO **DATA AS A CRITICAL ASSET**

Editor
Mark Deem

The Guide to Data as a Critical Asset 2022

Reproduced with permission from Law Business Research Ltd
This article was first published in April 2022
For further information please contact Natalie.Hacker@lbresearch.com

Published in the United Kingdom
by Global Data Review
Law Business Research Ltd
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.globaldatareview.com

To subscribe please contact subscriptions@globaldatareview.com

ISBN: 978-1-83862-859-8

Printed and distributed by Encompass Print Solutions
Tel: 0844 2480 112

Contents

Preface

Data is not just a source of regulatory risk: it is a vital asset for almost every type of organisation. Artificial intelligence and other forms of sophisticated computing and automation are no longer the stuff of science fiction: the future has become the present (or, at least, the near future). None of this would be possible without data. But even 'classic' business models now rely on the use of all forms of data, and its protection – whether in a data privacy or any other sense – is more important than ever.

Whether exploited as a core part of a business model, kept confidential during the development of a new product or processed with the care required by personal data regulation, information is now a board-level concern. GDR's *The Guide to Data as a Critical Asset* takes a unique view of data. Instead of looking at it through a regulatory and risk lens, the contributors to this book – edited by Mishcon de Reya partner Mark Deem – aim to steer companies through the gathering, exploitation and protection of all types of data, whether personal or not.

Global Data Review
London
March 2022

Accountability to Data Subjects and Regulators

Cédric Burton, Laura De Boel, Christopher N Olsen and Lydia B Parnes[1]
Wilson Sonsini Goodrich & Rosati

Introduction

In both the European Union and the United States, governments and data subjects may hold companies accountable for failure to maintain adequate privacy and security protections for their data assets. This article explores the similarities and differences between the EU approach, largely driven by Regulation (EU) 2016/679 (General Data Protection Regulation (GDPR)), and the US approach, largely driven by the Federal Trade Commission (FTC) and state law. Although the GDPR is theoretically a unifying statute with an express accountability principle, details about what constitute 'appropriate' measures continue to be worked out as the GDPR is applied. The FTC has developed its standards for privacy and data security through case-by-case enforcement over many years. Both the FTC and US state authorities rely on concepts such as 'reasonable' privacy and security measures that are fluid. Thus, companies are regularly held accountable in both jurisdictions, but compliance is no box-checking exercise. Companies that treat data as a critical asset are more likely to have the type of data governance framework in place that is needed to comply with accountability requirements.

---

1 Cédric Burton, Laura De Boel, Christopher N Olsen and Lydia B Parnes are partners at Wilson Sonsini Goodrich & Rosati (WSGR). The authors wish to acknowledge contributions to this article by Roberto Yunquera Sehwani, an associate in the Brussels office of WSGR, and Steve Schultze, an associate in the Washington, DC, office of WSGR.

Accountability under the GDPR

In the European Union, the principle of accountability is codified in Article 5(2) of the GDPR, which states that data controllers shall be 'responsible for, and be able to demonstrate compliance with' the GDPR's core principles. Accountability therefore entails two key elements: (1) the data controller is responsible for complying with the GDPR; and (2) the data controller must be able to demonstrate that it is compliant.[2] Although the principle is stated in simple terms, it is both broad and abstract. It is up to the individual data controller to decipher whether it has 'appropriate' measures in place to comply with all GDPR obligations and sufficient records to demonstrate that compliance.

Pre-GDPR, EU supervisory authorities (SAs) had advocated for the creation of an accountability principle to ensure that companies would take a proactive approach to their compliance with data protection laws.[3] SAs proposed the accountability principle so as to require companies to assess the data privacy and security risks posed by their activities and define the safeguards that would best mitigate those risks.[4] With the GDPR, the accountability principle became part of EU data protection law.

GDPR accountability in practice

Certain accountability measures for data assets are stipulated in the GDPR, such as record-keeping,[5] appointing a data protection officer (DPO)[6] and conducting data protection impact assessments (DPIAs).[7]

---

2 Information Commissioner's Office (ICO), Guide to the GDPR, 'Accountability and Governance', p. 1, at https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance-1-1.pdf (last accessed 9 Feb. 2022).

3 Article 29 Data Protection Working Party (WP29), 'Opinion 3/2010 on the principle of accountability' (Opinion 3/2010), para. 25.

4 'A provision on accountability would require data controllers to define and implement the necessary measures to ensure compliance with the principles and obligations of the Directive and to have their effectiveness verified periodically' – WP29 Opinion 3/2010, para. 39.

5 Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (GDPR), Article 30.

6 ibid., Article 37.

7 ibid., Article 35.

In addition, companies must take certain steps not expressly spelled out in the GDPR to comply with the accountability principle. For instance, large organisations will be expected to develop a comprehensive privacy management framework with dedicated staff, clear reporting lines, internal policies and procedures, and strong privacy safeguards embedded in their products or services.[8]

Organisations are typically expected to take the following measures to comply with the accountability principle.

Risk assessments and DPIAs

The GDPR requires companies to carry out a DPIA before conducting processing activities that may entail a high privacy risk. DPIAs must adhere to the structure set out in the DPIA Guidelines[9] of the European Data Protection Board (EDPB).[10] In addition to carrying out DPIAs for specific processing activities, organisations are expected to assess privacy risks throughout their operations. For instance, when outsourcing data processing to vendors, organisations should assess the privacy risks associated with vendor engagement.

Data protection officer

Although any organisation can choose to appoint a DPO, those that carry out certain privacy-sensitive processing operations on a large scale are required to appoint a DPO (e.g., large-scale profiling for credit scoring purposes). Companies should develop written policies and procedures to ensure the DPO's function is structured in accordance with the EDPB's Guidelines on DPOs.[11] In our experience, SAs often request companies to produce such documentation when they investigate an organisation, in particular to verify the DPO's independence within the organisation. Organisations need to comply with the GDPR's requirements on the designation, position and tasks

8 ICO, Guide to the GDPR, 'Accountability and Governance', p. 3.

9 'Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679', available at https://ec.europa.eu/newsroom/article29/items/611236 (last accessed 9 Feb. 2022).

10 The European Data Protection Board (EDPB) is an EU body that consists of all national supervisory authorities (SAs) in the European Union.

11 'Guidelines on Data Protection Officers ('DPOs')', available at https://ec.europa.eu/newsroom/article29/items/612048 (last accessed 9 Feb. 2022).

of the DPO even when the DPO is voluntarily appointed. Several SAs have already imposed fines on organisations that failed to demonstrate they had set up the DPO function in a compliant manner (see below).

Records of processing

The GDPR requires companies to keep records listing all data processing activities that they undertake. Records should be kept up to date and ready to be shared with SAs at their request. Several SAs have made template records available,[12] and they typically go beyond the information required by the GDPR. For instance, SAs' template records typically require companies to indicate the legal basis for data processing, which is not strictly required by the GDPR.[13] Companies should follow the guidance of the competent SA. SAs have already fined organisations for failure to have records of processing in place (see below).

Internal policies and procedures

Organisations are expected to implement internal policies and procedures regarding their data assets to ensure GDPR compliance in practice. Although the GDPR does not specify the issues that need to be addressed, typical policies and procedures include data handling policy, data breach handling policy, individuals' rights policy, data retention policy, data security policy and data protection audit procedure.

Training

Organisations should ensure that staff receive periodic training on privacy laws and the company's internal policies and procedures. Organisations should keep records of these training sessions to be able to demonstrate that they have implemented a comprehensive GDPR training programme.

---

12 For example, Belgian SA's template records, available at https://www.autoriteprotectiondonnees.be/professionnel/premiere-aide/toolbox; Italian SA's template records, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9047529; French SA's template records, available at https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement (web pages last accessed 9 Feb. 2022).

13 For example, Italian SA's template records, op. cit.; Polish SA's template records, available at https://uodo.gov.pl/pl/383/214 (last accessed 9 Feb. 2022).

Audit and review

The accountability principle also requires organisations to periodically review their approach to privacy compliance, to ensure that the implemented measures and safeguards remain appropriate in light of the privacy risks generated by the organisation's activities.

Codes of conduct and certification

The GDPR allows SAs to approve privacy codes of conduct and certificates to which companies could adhere. Adhering to an approved code of conduct or certification may serve to demonstrate a company's compliance with the accountability principle. However, few codes of conduct and certification schemes are currently available and adhering to a GDPR code of conduct or certification is not yet market practice.[14]

Enforcement of the GDPR accountability principle

Enforcement by supervisory authorities

Violation of the accountability principle is subject to the highest level of fines (i.e., €20 million (about US$24.35 million) or 4 per cent of the total worldwide annual turnover, whichever is higher). Several fines have already been imposed for violation of the accountability principle, albeit much lower. The following are some examples:

- The SA of Baden-Württemberg, Germany, imposed a fine of €300,000 for failure to provide adequate documentation concerning a vendor engagement. The company could not provide documentation identifying the types of personal data disclosed to the vendor, and the safeguards in place to protect the data.[15]

14 For example, the Belgian SA recently approved its first transnational code of conduct intended for cloud service providers (EU Cloud Code of Conduct) – more information available at https://www.dataprotectionauthority.be/citizen/the-be-dpa-approves-its-first-european-code-of-conduct. The EDPB keeps a public register for codes of conduct and for certification mechanisms, seals and marks, available at https://edpb.europa.eu/accountability-tools_en (web pages last accessed 9 Feb. 2022).

15 See FAQs at https://www.vfb.de/de/vfb/aktuell/neues/club/2021/fragen-und-antworten-zur-datenaffaere/ and press release of the data protection authority at https://www.baden-wuerttemberg.datenschutz.de/vfb-stuttgart-bussgeld-erlassen/ (web pages last accessed 9 Feb. 2022).

- The Greek SA imposed a fine of €150,000 on a company for failure to document its choice of legal basis for its processing activities. The SA determined that the company was not able to demonstrate how it complied with the GDPR's provisions concerning the legal basis for processing, which constituted a breach of the accountability principle.[16]
- The Italian SA imposed a fine of €30,000 for various violations, including failure to keep records of processing activities.[17]
- The Spanish SA imposed two fines of €50,000[18] and of €25,000[19] for failure to designate a DPO.
- The Belgian SA imposed a fine of €50,000 for failure to set up the DPO function in accordance with GDPR requirements.[20]

Compliance with the accountability principle does not prevent SAs from imposing fines for breach of other provisions of the GDPR.[21] However, SAs are likely to mitigate GDPR fines if an organisation keeps appropriate documentation, has strong privacy safeguards embedded in its products and services, and maintains clear privacy governance procedures.

Accountability and the one-stop shop mechanism

The accountability principle is a key part of the overall enforcement of the GDPR, especially in the context of the GDPR's one-stop shop mechanism (OSS). Under the OSS, a company's activities involving the processing of personal data across the European Union are subject to enforcement by the SA in the country where the company has its main EU establishment (e.g., the EU regional headquarters of a US multinational). That SA will be considered the 'Lead SA' and act as 'the sole interlocutor' of the

16 Greek SA, Decision 26/2019, summary available at https://edpb.europa.eu/sites/default/files/files/news/summary_of_decision_26_2019_en_2.pdf (last accessed 9 Feb. 2022).

17 Italian SA, Decision of 25 March 2021, available at https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9577323 (last accessed 9 Feb. 2022).

18 Spanish SA, Decision PS/00251/2020, available at https://www.aepd.es/es/documento/ps-00251-2020.pdf (last accessed 9 Feb. 2022).

19 Spanish SA, Decision PS/00417/2019, available at https://www.aepd.es/es/documento/ps-00417-2019.pdf (last accessed 9 Feb. 2022).

20 Belgian SA, Decision of 20 April 2020, available at https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-18-2020.pdf (last accessed 9 Feb. 2022).

21 WP29 Opinion 3/2010, para. 38.

company.[22] SAs often rely on the documentation kept to comply with accountability rules to determine which SA should be the Lead SA. For instance, SAs will check the location in which the DPO is based, or the office in which most policies and procedures relevant to privacy are adopted.[23] Companies should consider their approach towards the OSS when drafting their accountability documentation, to ensure that the documentation adequately reflects and justifies the company's approach.

Private enforcement: collective action lawsuits

The GDPR allows individuals and organisations to enforce the GDPR through the courts in EU Member States, using the accountability principle as a tool for litigation. The GDPR expressly grants individuals the 'right to an effective judicial remedy' before the courts of the Member State where the individual resides, in addition to any right to file complaints before SAs.[24] To facilitate the exercise of the right to an effective judicial remedy, the GDPR also allows non-profit organisations to submit complaints, including filing lawsuits in court, on behalf of multiple individuals.[25] The GDPR therefore provides for collective action lawsuits to be filed by non-profit organisations against companies.

Several private litigants (including collective action organisations) have argued that the accountability principle requires companies to proactively disclose information in court to demonstrate that the company is compliant with the GDPR. These litigants take the position that, under the accountability principle, individuals are not required to demonstrate that a company has breached the GDPR; rather that the company has to proactively demonstrate its compliance with the rules. The accountability principle, under this interpretation, reverses the burden of proof in court proceedings.

This approach has thus far been endorsed by courts only in a limited number of cases,[26] and it is not yet part of the case law of the European Court of Justice. In the cases where the accountability principle served to reverse the burden of proof, courts

22 GDPR, Article 56(6).

23 For instance, SAs will question a company's statement that their main EU establishment is in one country, if their data protection officer is located in another country and all the relevant policies governing data protection are drafted and adopted by employees based in another country.

24 GDPR, Article 79.

25 ibid., Article 80.

26 See, for instance, the judgment of Stuttgart Higher Regional Court in 'German court reverses GDPR burden of proof', *Global Data Review* (27 September 2021), at https://globaldatareview.com/data-privacy/german-court-reverses-gdpr-burden-of-proof (last accessed 9 Feb. 2022).

did not require plaintiffs to demonstrate that the defendant had breached the GDPR. Rather, they awarded damages to plaintiffs on the basis that the defendant companies had not been able to demonstrate that they complied with the GDPR. It is still unclear whether this will be the standard approach across the European Union. If so, this would constitute a significant change for litigants in continental Europe, where civil laws do not usually require defendants to disclose a vast amount of information, contrary to common law jurisdictions such as the United Kingdom or the United States, which have strict discovery rules.

Accountability in the United States

There is no uniform principle of accountability in the United States akin to the GDPR's Article 5(2). That is not to say that data controllers – in GDPR parlance – are unaccountable. On the contrary, companies are accountable to an overlapping patchwork of federal regulators, states and the data subjects themselves for proper handling of their data assets. The substantial accountability to each is discussed in the subsections below.

Accountability under EU and US law is not as different as it might first seem. Both jurisdictions leave much undefined. As described above, the broad and abstract language of the GDPR affords generous room for interpretation. Because the United States lacks any uniform legal code in this area, companies and data professionals have similarly improvised from the bottom up. As in the European Union, best practices are a surer lodestar of what companies may be held accountable for than any statute's text. More than a decade ago, leading academics explained that US privacy was governed far more by practices 'on the ground' than 'on the books'.[27] Little has changed in that regard. Although there have been perennial calls for unified data security and privacy legislation, none has emerged.[28] The result is an accretion of conventional wisdom endorsed by regulators or courts in the course of individual enforcement efforts.

27 Kenneth A Bamberger and Deirdre K Mulligan (2011), 'Privacy on the Books and on the Ground', *Stanford Law Review* 63: 247–315.

28 This article does not address the specialist statutes codifying liability for data protection failures in specific fields such as the Health Insurance Portability and Accountability Act for healthcare, Gramm Leach Bliley Act for financial services, and the Federal Information Security Management Act for federal agencies. Although those also incorporate reasonableness and other broad principles, they have considerably more detailed implementing regulations better suited for specialised review and have no applicability to entities outside their narrow spheres.

In the United States, 'reasonable' is a key term. For example, companies may represent in privacy policies or elsewhere that they 'take reasonable precautions and follow industry best practices' to ensure that data is not inappropriately 'lost, misused, accessed, disclosed, altered or destroyed'.[29] The US Federal Trade Commission (FTC) frequently holds companies accountable for failure to take reasonable measures, relying on industry practice to argue that their practice was unreasonable.[30] A growing number of state laws also require 'reasonable' measures to protect personal information independent of the company's representations. Under California law (a bellwether regime that applies broadly to many businesses that happen to serve California users), unreasonable practices are actionable by both the state attorney general and by individuals affected.[31] Such state laws generally do not define what is reasonable. Practitioners, regulators and enforcers have filled the void with case-by-case interpretations that become persuasive in future actions. There has thereby emerged a rough sense of which privacy and data security practices a company can be held accountable for to federal enforcers, state enforcers and individuals.

The federal government, through the FTC, has historically been the most active enforcer. But legal actions by state regulators and attorneys general also make up a substantial portion of enforcement activity, while actions by individuals through both traditional common law means and new state-level statutory grants of authority are common.[32] Unlike EU law, US law has no concept of a one-stop shop. Nor is there statutory federal pre-emption, generally. Thus, companies can be held accountable by each type of enforcer independently.

29 See, e.g., *Tapplock, Inc.*, File No. 1923011 (F.T.C. May 18, 2020) (complaint), https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockcomplaint.pdf (last accessed 9 Feb. 2022).

30 See, e.g., *Tapplock, Inc.*, File No. 1923011 (F.T.C. May 18, 2020) (decision and order), https://www.ftc.gov/system/files/documents/cases/1923011c4718tapplockorder.pdf (last accessed 9 Feb. 2022).

31 See Cal. Civ. Code § 1798.81.5 (requirement to implement and maintain reasonable security procedures, enforceable by the attorney general) and § 1798.150 (consumers may sue for breaches that result from unreasonable practices).

32 See, e.g., the Illinois Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14/1 et seq.

Accountability to the US Federal Trade Commission

The FTC is the most prominent US enforcer of data protection practices. It holds companies accountable even though it has no express statutory grant of sweeping authority over data security and privacy.[33] Instead, the FTC usually relies on its broad authority to police 'unfair or deceptive acts or practices in or affecting commerce' granted in Section 5 of the FTC Act.[34] It can do so (1) through an administrative proceeding directly under Section 5 or (2) as a lawsuit in federal district court under Section 13 as an actual or imminent violation of a 'provision of law enforced by the Federal Trade Commission'.[35] Some academics have described the FTC's case-by-case elaboration of its authority as a 'common law of privacy',[36] but that view is not universal. Much of this 'common law' consists of consent orders that are the result of negotiated settlements between the FTC and companies, as opposed to a court's legal determination after an adversarial process. The FTC's 'deception' authority is generally the most straightforward: a company that makes a privacy or data security commitment must honour it. These commitments are often made in privacy policies or in statements required by regulators but can also take the form of voluntary assertions. The FTC's authority over 'unfair' privacy or data security practices is more nuanced. And courts themselves have not been consistent with respect to the scope of the FTC's authority in this area. But in practice, those court decisions have not slowed the FTC's enforcement efforts.

---

33 Although the Federal Trade Commission (FTC) does not have an express statutory grant to enforce data protection or privacy writ large, some statutes do grant specific authority over narrow areas, such as children's privacy under the Children's Online Privacy Protection Act. 15 U.S.C. § 6501 et seq. The FTC recently announced that it will be embarking on a privacy rulemaking; as a result, we may see more specific privacy requirements in the future.

34 15 U.S.C. § 45(a).

35 15 U.S.C. § 53(b). Until recently, the FTC could seek monetary damages under Section 13(b) that were not available under Section 5(b). However, the United States Supreme Court held in *AMG Capital Management, LLC v. FTC*, 141 S. Ct. 1341 (U.S. 2021), that monetary damages were not available under Section 13(b) either. Unless the US Congress expressly grants this authority under one of the statutory provisions, first-time violators may be able to escape monetary relief. See Christopher Olsen and Stephen Schultze, 'FTC Authority Under Siege: Monetary and Injunctive Relief at Risk in Courts as Congress Contemplates a Response', 1, *Antitrust Source* (April 2021).

36 See Daniel J Solove and Woodrow Hartzog, 'The FTC and the New Common Law of Privacy', 114 *Columbia Law Review* 583 (2014).

The first important decision regarding FTC authority for data security accountability came in 2015 from the United States Court of Appeals for the Third Circuit. In *FTC v. Wyndham Worldwide Corporation*, the Court held that the FTC could proceed against Wyndham under its 'unfairness' authority for failure to encrypt customer information, to enforce strong passwords or to employ reasonable measures to detect and prevent unauthorised access, among other things.[37] Wyndham had suffered multiple security breaches and the FTC's list of alleged failures was long. The FTC argued that each of the specific failures was unfair under the terms of the statute. The Court noted that the FTC might also have the authority to pursue a claim that Wyndham had acted deceptively by violating its general promise to use commercially reasonable measures that, according to its privacy policy, included vague 'appropriate safeguards'. The Court ultimately concluded that Wyndham's alleged failures were plainly 'unfair' under the statute.[38] It also rejected Wyndham's argument that without notice of what specific practices were required, the company lacked fair notice of what it must do to comply with the statute.[39]

The second important decision appeared to cut the other way, although it did not directly conflict with *Wyndham*. In 2018, the United States Court of Appeals for the Eleventh Circuit held in *FTC v. LabMD* that an FTC order requiring the company to implement 'reasonable safeguards' was too vague to be enforceable under the statute.[40] The FTC's order, according to the court, 'command[ed] LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness'.[41] Commentators noted that if, according to the Eleventh Circuit, a court cannot determine what constitutes a reasonable data security or privacy regime for the purpose of enforcing an injunctive order, then a court should likewise be unable to determine whether a regime is reasonable from the perspective of the statute itself. But the *LabMD* decision did not cite the *Wyndham* decision and instead avoided addressing the issue, so there was no clear procedural path for the United States Supreme Court to resolve the apparent split between the Third and Eleventh circuits. For its part, the FTC revised its subsequent data security orders to add more specific requirements.[42]

---

37 *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240–41 (3d Cir. 2015).

38 ibid., at 244–47.

39 ibid., at 255–59.

40 *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1237, 1241 (11th Cir. 2018).

41 ibid., at 1246.

42 https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance (last accessed 9 Feb. 2022).

The practical effect is that companies must assume that the FTC has broad authority to bring enforcement actions for allegedly unreasonable privacy or data security practices – whether directly under the statute's 'unfair or deceptive' prohibition, as violation of a privacy policy's 'reasonableness' promise, or as a violation of an existing order requiring 'reasonable' measures. Facebook experienced this dynamic in 2019 when the FTC alleged that the company had been giving third parties access to certain user data, contrary to the company's public statements and contrary to a 2012 consent order that required both specific safeguards and implementation of a 'comprehensive privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information'.[43] The FTC's US$5 billion settlement, while subject to much debate, was at least a demonstration of the FTC's practical authority to hold companies accountable for maintaining 'reasonable' privacy and data security protections.

Zoom found itself in a similar position in November 2020 when the FTC alleged that the company deceptively failed to implement several encryption measures that it claimed existed.[44] Above and beyond the company's failure to live up to its express promises about encryption, the FTC alleged that the company's software unfairly 'circumvent[ed] a security and privacy safeguard' built into the Safari web browser. Notably, the FTC explicitly alleged that this unfair security and privacy practice harmed consumers and it identified no countervailing consumer benefit.[45]

The Sedona Conference, an influential collection of judges, practitioners and academics, has surveyed the standards that courts, regulators and practitioners might use to determine what constitutes reasonable data security.[46] The Sedona Conference authors first observed that *Wyndham* quoted the FTC's statutory authority to hold an act or practice unfair when it 'causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition'.[47] That formulation, the authors noted, is akin to the classic cost/benefit reasonableness test for tort liability

43 See *In re Facebook, Inc.*, Dkt. No. C-4365, 2012 FTC LEXIS 135, *9 (F.T.C, Jul. 27, 2012), *In re Facebook, Inc.*, 2020, Dkt. No. C-4365, FTC LEXIS 80, *16–19 (F.T.C., Apr. 27, 2020).

44 *In re Zoom Video Comm'cns, Inc.*, 2020 WL 6589816 (F.T.C., Nov. 9, 2020) (complaint).

45 ibid., at ¶ 38.

46 See The Sedona Conference, 'Commentary on a Reasonable Security Test', 22 *Sedona Conference Journal* 345 (2021).

47 ibid., at 376 (quoting *Wyndham*, 799 F.3d at 255–59).

articulated by Judge Learned Hand in *United States v. Carroll Towing Co*.[48] Further extending their common law analogy, the authors also highlighted the role of industry custom and cost/benefit calculations in determining whether an actionable products liability tort occurred. This way of defining reasonableness in the privacy and data security context likely resonates with common law practitioners. Absent a prescriptive statute, it may be the closest thing to a general legal standard that exists.

In practice, companies that wish to avoid being held accountable to the FTC must digest prior FTC cases and consent decrees, FTC guidance and industry standards to determine what measures to implement. For example, *Wyndham* highlighted encryption of stored data, network monitoring for malware, password complexity, proper use of firewalls and intrusion detection.[49] The initial 2012 Facebook consent order is an example of a privacy regime that the FTC considered appropriate for a large company that was a first-time violator: implementation of a comprehensive privacy programme with 'reasonable' safeguards, biennial assessment by an independent third party and reporting to the FTC, and changes tailored to the specific failure. The 2019/2020 Facebook consent order is an example of a privacy regime that the FTC considers reasonable for a recidivist: appointment of board-level privacy compliance officers, enhanced transparency measures, pre-launch product functionality privacy review, proactive breach reporting and a substantial monetary penalty.[50] The FTC also provides high-level guides for protecting personal information and implementing security protections.[51] Overviews such as the Sedona Conference commentary catalogue some of the most salient industry standards, including the Center for Internet Security Critical Survey Controls (CIS Controls)[52] and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).[53]

---

48 159 F.2d 169, 173 (2d Cir. 1947.

49 *Wyndham*, 799 F.3d at 258–59.

50 *In re Facebook, Inc.*, 2020, Dkt. No. C-4365, FTC LEXIS 80, (F.T.C., Apr. 27, 2020).

51 FTC, 'Protecting Personal Information: A Guide for Business' (2016), at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf; FTC, 'Start with Security: A Guide for Business' (2015), at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (web pages last accessed 9 Feb. 2022).

52 Center for Internet Security, CIS Critical Security Controls, at https://www.cisecurity.org/controls/ (last accessed 9 Feb. 2022).

53 National Institute of Standards and Technology, Cybersecurity Framework, https://www.nist.gov/cyberframework (last accessed 9 Feb. 2022).

Accountability to the states

Many states have laws that give state regulators or the state authority to hold companies accountable for privacy and data protection. These laws are diverse but fall into two broad categories. The first type of law requires businesses to notify consumers or regulators (or both) of data breaches. The definition of 'breach' (or even whether the state's law uses the term 'breach') differs by state. Lawyers advising a company that has suffered a breach will typically first gather the facts about the nature of the breach and the population affected, then analyse those facts against a complex matrix of state laws. There are basic matrices published by the National Conference of State Legislatures and the International Association of Privacy Professionals.[54] The second type of law requires businesses to maintain reasonable privacy and data protection practices. These laws are even more diverse and range from specific privacy and security statutes with implementing regulations to general consumer protection statutes.

New York and California are good examples. Section 899-AA of the New York General Business Law governs breach notification, and Section 899-BB governs data security protections. Section 899-AA requires notification when defined 'private information' is breached, and lays out several factors that a business may consider when determining whether the information has been 'acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization' (i.e., breached). Section 899-BB requires 'reasonable safeguards to protect the security, confidentiality and integrity of the private information'. The provisions are enforceable by the state, and do not create a private right of action. Section 1798.82, and related sections, of the California Civil Code requires breach notification in a specific format and creates a private right of action for failure to notify. Section 1798.81.5 of the Code requires companies to 'implement and maintain reasonable security procedures' and is enforceable by the California Attorney General.

In 2016, California's then Attorney General, Kamala Harris, published a data breach report that included a series of recommendations. Like the FTC guides, these recommendations indicate what a state might consider to be reasonable privacy and data security protections. The Attorney General described 'reasonable security' as 'the

54 See National Conference of State Legislatures, 'Security Breach Notification Laws', https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx; International Association of Privacy Professionals, 'State Data Breach Notification Chart', https://iapp.org/resources/article/state-data-breach-notification-chart/ (web pages last accessed 9 Feb. 2022).

standard of care for personal information'.[55] This first suggests that the CIS Controls are the baseline minimum standard of care.[56] The report also recommend multi-factor authentication,[57] encryption of data in transit[58] and fraud alerts.[59] The report concludes by acknowledging that state laws differ, but calls for increased efforts to harmonise state laws rather than pre-empting them through a uniform federal law.[60]

Notwithstanding the Attorney General's call for harmonisation, state laws have only become more diverse. California itself has been promulgating new statutes and regulations at a rapid pace, with much still unsettled in practice. The 2018 California Consumer Privacy Act added a host of new requirements, including Civil Code Section 1798.150, which gives consumers the right to sue directly for breaches arising from unreasonable security practices. The 2020 California Privacy Rights Act created a new state regulatory agency, the California Privacy Protection Agency, with rule-making authority and independent power to investigate and prosecute violations. Many of the details about what the Agency will do and how it will work remain to be determined before and after it becomes operational in 2023. The Act itself outlines seven high-level responsibilities of businesses that cover data collection, notice, deletion, correction and a requirement to 'take reasonable precautions to protect consumers' personal information from a security breach'.

Thus, the trend at the state level is to increase accountability to states by both promulgating more requirements and creating additional – and sometimes indeterminate frameworks – premised on what is 'reasonable'. Although the states may not be focused on harmonisation and the federal government may not pass unifying privacy and data security statutes in the foreseeable future, businesses that follow prior state enforcement actions, written guidance and generally accepted industry practice can best satisfy diverse state accountability standards.

55 Kamala D Harris, California Dep't of Justice, 'California Data Breach Report' (February 2016), *27, at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (last accessed 9 Feb. 2022).

56 ibid., at 30.

57 ibid., at 34.

58 ibid., at 36.

59 ibid., at 37.

60 ibid., at 38.

Accountability to data subjects in the United States

Data subjects may bring an action in the United States either as an individual or as a class. They may do so under express state causes of action or common law tort. Any privacy or data breach action of this sort is likely to face several early procedural and jurisdictional hurdles, including removal to federal court or remand to state court, class certification objections, attempts to consolidate via multi-district litigation and challenges to standing. There are few cases that have proceeded to the merits and defined the specific practices for which data subjects can hold companies accountable.

Individual and class suits typically require highly specialised plaintiffs' and defendants' lawyers. The myriad procedural and jurisdictional questions generally make them large and complex undertakings that are frequently structured as multistate class actions in federal court. Much of the dispute in these cases involves whether the action qualifies as a 'case or controversy' under the Article III of the US Constitution.[61] In a string of cases, the US Supreme Court has held that for data inaccuracies or disclosures to constitute a case or controversy, plaintiffs must plead an 'injury in fact' that is sufficiently specific to show that they were harmed or faced imminent harm.[62] This is a complex and fact-specific area of law. Most suits are either dismissed at or before a standing challenge; otherwise they generally survive and are settled.

The 2017 Equifax data breach provides a case study of all modes of US accountability operating simultaneously. Indeed, had the breach occurred after the GDPR came into effect, the company might have faced EU accountability as well. The plaintiffs' bar seized upon the opportunity to sue Equifax even before regulators became publicly involved. In typical fashion, many class actions were initiated nationwide, consolidated in multi-district litigation and challenged together in a motion to dismiss.[63] The plaintiffs' theories included negligence, violation of state consumer protection and fraud laws, and violation of state data breach notification laws.[64] All survived the motion to dismiss, at least in part.[65] Shortly thereafter, Equifax settled with the consumer class

61 U.S. Const. art. III, § 1, cl. 1.

62 See *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016); *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2211–13 (2021).

63 *In re Equifax, Inc.*, 362 F. Supp. 3d 1295, 1308–11 (N.D. Ga. 2019). Somewhat uncharacteristically, Equifax did not contest standing. ibid., at n. 70.

64 ibid., at 1321–43.

65 ibid., at 1345.

for about US$380 million.[66] During the same period, the FTC, the federal Consumer Financial Protection Bureau and state attorneys general conducted their own investigations under their own authorities.[67] These culminated in a coordinated settlement for about US$575 million independent of the consumer class action.[68] Although few privacy and data security failures will garner as much attention as the Equifax data breach, the incident serves as a reminder that accountability in the United States can come from all enforcers at once.

66 See Order Granting Final Approval of Settlement, Certifying Settlement Class, and Awarding Attorney's Fees, Expenses and Service Awards, *In re: Equifax Inc. Customer Data Security Breach Litigation*, No. 1:17-md-02800-TWT (N.D. Ga. Jan. 13, 2020), ECF No. 956.

67 See 'Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach', FTC (Jul. 22, 2019), at https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related (last accessed 9 Feb. 2022).

68 id.

CÉDRIC BURTON
Wilson Sonsini Goodrich & Rosati

Cédric Burton is a leader in Wilson Sonsini's Brussels office, where he co-leads the firm's global privacy and cybersecurity practice and leads the EU data protection team. He assists clients of all sizes with regard to privacy and data protection, information technology, data security, advertising and marketing, and e-commerce laws.

Cédric has developed substantial experience in advising companies on all facets of global, European and Belgian privacy and data protection law. His privacy and data protection practice covers all sectors and includes a wide range of activities, such as defining global pan-European strategies for compliance, developing creative and practical advice on unsettled topics, such as online profiling and behavioural advertising, counselling clients on how to resolve or mitigate risks relating to conflicts between EU data protection law and foreign requirements, and representing clients in their dealings with the European Commission and other major regulatory bodies.

Cédric has authored many articles on privacy and data protection law and speaks regularly on data protection-related topics. Prior to Wilson Sonsini, he worked as a research fellow in privacy and data protection law at the Research Center on IT and Law (CRID) of the University of Namur (Belgium) and at the Center on Law and Information Policy at Fordham University (New York).

LAURA DE BOEL
Wilson Sonsini Goodrich & Rosati

Laura De Boel is a partner in the Brussels office of Wilson Sonsini Goodrich & Rosati. Her practice is focused on all aspects of European data protection law, including data breaches, international data transfers and online profiling. She has extensive experience in advising clients on pan-European data protection compliance across a range of sectors. She also assists clients in their dealings with privacy and data protection authorities, such as the Belgian Privacy Commission.

Laura has been quoted in leading industry and legal publications, including Bloomberg BNA. She is a native Dutch speaker and is fluent in English and French.

CHRISTOPHER N OLSEN
Wilson Sonsini Goodrich & Rosati

Christopher Olsen advises clients on all aspects of privacy and cybersecurity matters and represents companies under investigation by the Federal Trade Commission and state attorneys general. He has an established track record of success in resolving investigations without enforcement action and clients regularly seek his guidance when facing high-stakes regulatory scrutiny.

Chris is a former deputy director of the Bureau of Consumer Protection at the Federal Trade Commission (FTC), where he directed the international work of the Division of Privacy and Identity Protection and acted as the agency's co-lead negotiator in discussions with the European Commission regarding improvements to and renewal of the US–EU Safe Harbor Framework.

Prior to joining the bureau director's office, Chris was the assistant director of the Division of Privacy and Identity Protection at the FTC. In this role, he managed a number of significant privacy and security enforcement actions, as well as several of the most important privacy initiatives in recent FTC history, including a seminal 2012 FTC report on consumer privacy that formulated important recommendations for businesses.

LYDIA B PARNES
Wilson Sonsini Goodrich & Rosati

Lydia Parnes is a partner in the Washington, DC, office of Wilson Sonsini Goodrich & Rosati, where she is co-leader of the firm's privacy and cybersecurity practice. She regularly represents companies in complex regulatory investigations and provides advice on complying with federal, state, and global privacy and data protection laws.

The former director of the Bureau of Consumer Protection (BCP) at the Federal Trade Commission (FTC), Lydia is a highly regarded privacy expert. As director of the BCP, Lydia oversaw privacy and data security enforcement efforts and the development of the FTC's approach to online advertising. She testified on numerous occasions on the benefits of a uniform nationwide data breach law and the risks of legislating in the technology area.

Lydia advises companies on how to navigate global privacy and data security requirements while pursuing their business goals. She helps them develop and implement comprehensive privacy compliance programmes and understand the nuances of regulation and self-regulation in the privacy arena. Lydia regularly represents clients before the FTC and other federal and state agencies.

Lydia is regularly recognised among the country's top privacy and data security attorneys in *Chambers USA*, *Chambers Global* and *Who's Who Legal: Business Lawyers*.

WILSON SONSINI

As the premier legal adviser to technology, life sciences and growth enterprises worldwide, Wilson Sonsini is at the forefront of privacy and cybersecurity law in the United States and throughout the world. Our cross-disciplinary team of highly experienced professionals helps companies navigate the complex and ever-changing set of laws, regulations and industry standards that govern the collection, storage and use of information.

Our privacy and cybersecurity team includes former senior officials who served in the Federal Trade Commission's Bureau of Consumer Protection, the US Department of Justice's National Security Division and the Department of Homeland Security. The team also includes some of the nation's leading litigators and veteran trial attorneys who have litigated complex data disputes involving novel issues of law. Rounding out the team are compliance and transactional attorneys, as well as legislative and regulatory strategists.

Rue Montoyer 47
Brussels, 1000
Belgium
Tel: +32 2 274 57 00

1700 K Street NW
Fifth Floor
Washington, DC 20006
United States
Tel: +1 202 973 8800

www.wsgr.com

Cédric Burton
cburton@wsgr.com

Laura De Boel
ldeboel@wsgr.com

Christopher N Olsen
colsen@wsgr.com

Lydia B Parnes
lparnes@wsgr.com

Data is not just a source of regulatory risk: it is a vital asset for almost every type of organisation. Whether exploited as a core part of a business model, kept confidential during the development of a new product or processed with the care required by personal data regulation, information is now a board-level concern. GDR's *The Guide to Data as a Critical Asset*, edited by Mishcon de Reya partner Mark Deem, offers a unique approach to data that helps steer companies through their gathering, exploitation and protection of all types of data – whether personal or not – and looks at data as an asset class that is increasingly important across all industries.

Visit globaldatareview.com
Follow @GDR_alerts on Twitter
Find us on LinkedIn

ISBN 978-1-83862-859-8