BORN IN THE USA: THE GDPR AND THE CASE FOR TRANSATLANTIC PRIVACY CONVERGENCE

GABE MALDOFF* & OMER TENE**

INTRODUCTION

The European-US privacy divergence is well-documented. Since the development of data protection laws in Europe in the 1970s, through the scuffles over PNR, SWIFT, and adequacy up until the very public post-Snowden fallout resulting in the invalidation of Safe Harbour in 2015, the continents appear to be diverging inexorably, slow and unstoppable as tectonic drift. Europe's new General Data Protection Regulation (GDPR) is the latest landmark.[1]

When it came into effect, the GDPR imposed a litany of specific requirements on organizations that process the personal data of individuals in the European Union (EU). It is an approach seemingly at odds with the sectoral and harms-based framework in the US. While the GDPR will grant protections to US and other non-Europeans whose data is processed in the EU, the US has moved to explicitly limit the application of its government privacy

* Gabe Maldoff is an Associate at Covington & Burling LLP and a former Westin Fellow at the International Association of Privacy Professionals,

** Omer Tene is Vice President and Chief Knowledge Officer at the International Association of Privacy Professionals.

1. Council Regulation 2016/679, 2016 O.J. (L 119) 1 [hereinafter GDPR].

laws to foreign residents. Even amidst the Cambridge Analytica-Facebook saga, the chance of a comprehensive US data protection regime emerging in Washington to counter GDPR remains remote. Many of Mark Zuckerberg's congressional inquisitors could hardly agree on what the issue was they were trying to tackle, let alone how to solve it.

The continuing discord over data transfers and government access would have you thinking that when it comes to privacy, the Americans are from Mars and the Europeans from Venus. But this narrative misses an important plotline in the story of transatlantic privacy protections. Perhaps counterintuitively, from fundamental constitutional formulations to an emphasis on accountability and special protections for children's data, many of the GDPR's legal innovations draw directly from US legal sources, jurisprudence, and experience. The result is a transatlantic approach to privacy, as much American as it is European, that aims to translate privacy protections from words to concrete action. Seen through these lenses, rather than being polar opposites, the US and the EU share and mutually draw upon many common underlying principles of privacy law.

I. "REASONABLE EXPECTATION OF PRIVACY" AND "CONTEXT"

Although the US Constitution does not explicitly mention privacy, the Supreme Court has repeatedly recognized certain "zones of privacy" within the constitutional text.[2] In *Katz v. United States*,[3] relying on these broader notions of privacy, the Supreme Court extended Fourth Amendment protections beyond private property, to "people, not places."[4] Justice Harlan's concurrence in that case articulated the enduring standard against which to measure government searches and seizures. He asked whether the search intruded upon a person's "*reasonable expectation of privacy*."[5]

In addition to governing the development of Fourth Amendment doctrine, Justice Harlan's formulation has had influence beyond the US. In 1984, the Canadian Supreme Court adopted the reasonable expectation of privacy test in interpreting the Canadian Charter, after discussing the *Katz* decision at length.[6] The formulation also appeared in several cases from the European Court of Human Rights beginning in the late 1990s.[7]

2. Griswold v. Connecticut, 381 U.S. 479, 484 (1965); *see also* Carey v. Population Serv. Int'l, 431 U.S. 678, 684 (1977).

3. 389 U.S. 347 (1967).

4. *Id.* at 351.

5. *Id.* at 360 (Harlan, J., concurring).

6. Hunter et al. v. Southam Inc., [1984] 2 S.C.R. 145, 158–59 (Can.).

7. Uzun v. Germany, App. No. 35623/05, Eur. Ct. H.R. (2010); Peck v. United Kingdom, App. No. 44647/98, 36 Eur. Ct. H.R. (2003); P.G. v. United Kingdom, App. No.

An assessment of individuals' reasonable expectations of privacy has influenced protections in academic discourse too. In *Privacy in Context*, Helen Nissenbaum argued that privacy issues arise any time information is used in a different context from that in which the information was given. Thus, privacy depends on information norms, which in turn derive from the reasonable expectations of data subjects.[8] This view influenced the Federal Trade Commission's efforts to protect consumer privacy.[9] In its 2012 guidance, the FTC urged companies to provide users with enhanced notice of any data practices that are not "commonly accepted."[10]

By contrast, before the GDPR, reasonable expectations and contextual analysis were largely absent from European data protection. The EU Data Protection Directive contains little trace of either concept.[11] In this regard, the GDPR marks a significant departure from the Directive in favor of the US intellectual tradition. Under the GDPR, as described in further detail below, reasonable expectations will come to define the important balancing act between the legitimate interests of the controller and countervailing rights of individual data subjects. Context will play an even greater role, in multiple GDPR sections ranging from how to provide notice of processing to how to implement appropriate data security measures. By embracing context and individual expectations, European policymakers introduced a subjective and evolutionary factor into the heart of their framework, which has traditionally been characterized by rigid, top-down rules. In line with American jurisprudence and scholarship, the analysis of privacy rights must now evolve flexibly to meet changing social norms.

A. A New Model of Choice Based on Reasonable Expectations

The GDPR, like the Directive before it, forbids organizations from processing personal data without first identifying a lawful basis. Lawful bases include the consent of the individual whose

44787/98, Eur. Ct. H.R. (2001); Halford v. United Kingdom, App. No. 20605/92, 24 Eur. H.R. Rep. 523 (1997).

8. HELEN NISSENBAUM, PRIVACY IN CONTEXT 129–52 (1st ed. 2010).

9. Alexis C. Madrigal, *The Philosopher Whose Fingerprints Are All Over the FTC's New Approach to Privacy*, ATLANTIC (Mar. 29, 2012), https://www.theatlantic.com/technology/archive/2012/03/the-philosopher-whose-fingerprints-are-all-over-the-ftcs-new-approach-to-privacy/254365/ [https://perma.cc/C3RD-9NZH].

10. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 38 (2012) [hereinafter FTC REPORT], https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/B8MZ-KFJP].

11. Council Directive 95/46/EC, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

data is being processed, or, alternatively, a legal requirement in the EU, public interest, or "the legitimate interests pursued by the controller. . . ."[12] A controller or a third party may rely on its legitimate interests to process personal data, unless "such interests are overridden by the interests or fundamental rights and freedoms of the data subject. . . ."[13]

The analysis of legitimate interests, as articulated in Preamble 47, must "tak[e] into consideration the reasonable expectations of data subjects based on their relationship with the controller."[14] The controller must assess, in light of the circumstances, "whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place."[15]

The reasonable expectation of privacy test, originally articulated in Justice Harlan's concurrence in *Katz*, is thus poised to play an outsized role under the GDPR. As the Regulation imposes greater constraints on consent as a legal basis, organizations are increasingly likely to rely on their legitimate interests for processing personal data.[16] The result is an American-flavored version of individual choice that is more nuanced than the traditionally stiff consent requirements of the EU framework. Under this model, controllers will rely on their legitimate interests where processing aligns with the reasonable expectations of data subjects;[17] whereas data subjects will be able to choose whether to permit any processing that exceeds those expectations.[18]

Under the GDPR, some of the most data-rich processing activities within organizations, like research and development and any kind of reactive data modelling (central to the development of artificial intelligence and machine learning algorithms), will likely be governed by the "reasonable expectations" standard. This is because the GDPR generally restricts data processing to only the specific purposes for which the data was initially collected.[19] An organization may use personal data for different purposes only if the secondary processing is compatible with the initial one.[20]

Data analysis and research are rarely the primary purpose for which personal data is collected. Indeed, organizations would

12. GDPR, *supra* note 1, art. 6(1)(f).
13. *Id.*
14. *Id.* pmbl. 47.
15. *Id.*
16. Omer Tene & Christopher Wolf, The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent 2 (2013) (unpublished manuscript), https://www.scribd.com/document/121642539/The-Draft-EU-General-Data-Protection-Regulation-Costs-and-Paradoxes-of-Explicit-Consent [https://perma.cc/DZ6N-U2MK].
17. *Legitimate Interest*, GDPR EU.ORG, https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/ [https://perma.cc/B5DN-UPH7].
18. *See generally* GDPR, supra note 1.
19. *Id.* art. 5(1).
20. *Id.* pmbl. 50.

struggle to even meaningfully explain big data analysis and machine learning to data subjects. To meet the test of compatibility under the GDPR, an organization must consider a number of factors, including the link between the initial and secondary purposes, the nature of the data, the possible consequences of processing, as well as "the context in which personal data have been collected, in particular the reasonable expectations of data subjects. . . ."[21] A controller's ability to conduct further processing, including under the expansive research provisions of the GDPR, will therefore depend on *context* and consumer expectations.

B. The GDPR Embraces Contextual Privacy

The word "context" appears 57 times in the Regulation,[22] compared to only six times in the Directive.[23] But it is not just the frequency of its use that is striking. The way in which the Regulation breathes life into the term and applies it in myriad settings emulates the contextual approach pioneered by American legal scholars, such as Nissenbaum, and followed by the US Administration and federal regulator, the Federal Trade Commission (FTC).

The most vivid example is how context informs the Regulation's notice provisions. The Regulation requires controllers to "take appropriate measures" to communicate with data subjects about their rights and the controller's processing activities.[24] Preamble 60 adds that a controller's notice to the data subject "should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed."[25] Like the FTC's approach, which encourages different forms of notice depending on the context of the collection, the GDPR suggests that notice should be specific to the context in order to ensure effective communication of data practices. The result is that both the content and the form of the notice—for example, is it bundled in a broader policy or is it delivered just in time for a particular use?—depend on the context of each transaction.

The use of context in this setting helps to resolve one of the challenges presented in the GDPR. Article 12 states that notice must be presented "in a concise, transparent, intelligible and easily accessible form."[26] At the same time, the list of items of information

21. *Id.*
22. *See id.*
23. *See* Data Protection Directive, *supra* note 11.
24. GDPR, *supra* note 1, art. 12(1).
25. *Id.* pmbl. 60.
26. *Id.* art. 12(1).

required in a notice, specified in Article 13, spans more than two pages of the Regulation.[27] To address the tension between these requirements, for specificity, granularity and brevity, the Article 29 Working Party's guidelines on transparency recommended adopting a "layered" approach, to help provide the most relevant information in a manner adapted to the context of a transaction.[28] By relying on this approach, a controller can provide enhanced notice of any practices that exceed a user's reasonable expectations, while providing greater detail of the controller's data practices in a longer form elsewhere.

More broadly, contextual analysis is at the heart of the Regulation's "risk-based approach"—which itself marks a significant departure from the Directive and an adoption of US norms. In sections ranging from the responsibilities of the controller for complying with the Regulation and implementing appropriate data security to the provisions that govern privacy by design and privacy impact assessments, the Regulation requires controllers to tailor their practices to the assessed degree of privacy risks. Understanding risk necessarily (and explicitly) requires controllers to consider "the nature, scope, context and purposes of processing."[29]

Finally, contextual analysis pervades the Regulation's provisions that relate to automated decision-making and profiling, which are poised to play a greater role as organizations increasingly rely on algorithmic engines to power decisions and recommendations. Where a controller engages in such processing, it must "implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests. . . ."[30] Such measures must be designed to minimize the risk of errors and discriminatory effects, "taking into account the specific circumstances and context in which the personal data are processed."[31] In these crucial provisions, which going forward will form the backstop against the most dangerous side effects of advanced computing, the European framework embraced the American formulation of contextual analysis and risk measurement over the rigid rules that previously characterized the European regime.

II. ACCOUNTABILITY

The concept of accountability derives from the 1980 Organization for Economic Cooperation and Development (OECD)

27. *See id.* art. 13.
28. *See id.* art. 29.
29. *See, e.g.*, *id.* arts. 24(1), 25(1), 32(1), 35(1), 39(2).
30. *Id.* art. 22(3).
31. *Id.* pmbl. 71.

Privacy Guidelines,[32] the first international effort to create a unified approach to privacy regulation. Under the OECD's accountability principle, "a data controller should be accountable for complying with measures which give effect to the principles stated above."[33] As further explained in the 2013 revisions to the OECD Guidelines, accountability means putting in place a privacy management program that is appropriate to the risks of an operation, provides for internal oversight and governance, includes plans for responding to inquiries and incidents, and is continuously updated and reviewed.[34]

Accountability has been a feature of Canadian privacy protections since 2000. In its 2012 accountability guidelines, the Office of the Privacy Commission of Canada explained that accountability is "the first among the principles because it is the means by which organizations are expected to give life to the rest of the fair information principles that are designed to appropriately handle and protect the personal information of individuals."[35]

In the US, even in the absence of formal legislation, accountability measures emerged within the private sector as a means of protecting brand reputation, respecting consumer expectations, and reducing risk. In the late 1990s, with the rise of information technology, an emphasis on enhancing trust in the nascent digital economy forced companies to devote internal resources toward protecting consumer expectations. Companies that failed to satisfactorily address the public's privacy concerns—such as AOL in its thwarted plan to sell phone numbers to marketers[36] or DoubleClick, which proposed to combine clickstream data with personally identifying information[37]—were met with public scorn.[38]

In the decade that followed, an entire industry emerged focused on managing privacy risks and creating accountable data governance measures. The International Association of Privacy

32. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, ORG. FOR ECON. CO-OPERATION & DEV. (1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/XA85-SWVD].

33. *Id.* art. 14.

34. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data art. 15, ORG. FOR ECON. CO-OPERATION & DEV. (2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf [https://perma.cc/4W33-D8UA].

35. OFFICE OF THE PRIVACY COMM'R OF CAN. ET AL., GETTING ACCOUNTABILITY RIGHT WITH A PRIVACY MANAGEMENT PROGRAM 3 (2012).

36. Seth Schiesel, *America Online Backs Off Plan To Give Out Phone Numbers*, N.Y. TIMES (July 25, 1997), https://nyti.ms/2VACnPT [https://perma.cc/CX87-DEL9].

37. Andrea Petersen, *DoubleClick Reverses Course After Outcry on Privacy Issue*, WALL ST. J. (Mar. 3, 2000, 9:53 AM), https://www.wsj.com/articles/SB952019045241548818 [https://perma.cc/3CUJ-DSFL].

38. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, 63 STAN. L. REV. 247, 282–84 (2010).

Professionals (IAPP), born in 2000 to serve the small but budding privacy profession, grew to ten thousand members in 2012 and more than forty thousand in 2018.[39] The privacy profession was dedicated to the bedrock principle underlying accountability—that the success of privacy protection depends not on the vindication of formulaic notice and consent but rather on securing the trust of those whose information is at stake through responsible data practices.[40]

US law followed, seeking to codify the consensus that already existed among those in the privacy profession. FTC enforcement actions through the 2000s focused on protecting consumer expectations by enforcing against consumer deception and unfairness.[41] Although not an explicit feature of the FTC Act, which dates back more than a century, accountability is depicted by the agency as "embodied in the FTC's framework. . . ."[42] Importantly, in dozens of enforcement actions in the field of privacy and data security, the FTC ordered companies to set up elaborate accountability programs for data governance, including external third party audits for periods up to 20 years. Additionally, the Obama Administration's proposed Consumer Privacy Bill of Rights in 2012 included explicit accountability measures.[43] Moreover, amendments to the Health Insurance Portability and Accountability Act in 2013 encoded several accountability mechanisms, including mandatory investigations of possible violations and penalties even for inadvertent violations in the health sector.[44]

In Europe, the GDPR for the first time formally introduced the concept of accountability into EU law, both as an explicit principle[45] and encoded in provisions throughout the Regulation. The GDPR requires controllers to "implement technical and organizational measures to ensure *and to be able to demonstrate* that processing is performed in accordance with the Regulation."[46] This includes a

39. Andrew Bolson, *Should Privacy Pros be Privacy Advocates?*, IAPP (June 22, 2018), http://iapp.org/news/a/should-privacy-pros-be-privacy-advocates [https://perma.cc/MTB2-8LM7].

40. *See* Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 902–03 (2013).

41. CHRIS J. HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 74–79 (1st ed. 2016).

42. FTC REPORT, *supra* note 10, at 10.

43. THE WHITE HOUSE, CONSUMER DATA IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1, 21–22, 48, 52 (2012), https://www.hsdl.org/?view&did=700959 [https://perma.cc/LJZ7-R7AL].

44. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at 45 C.F.R. §§ 160, 164 (2019)).

45. GDPR, *supra* note 1, art. 5(2) ("The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')").

46. *Id.* art 24(1).

requirement to maintain a detailed record of processing activities[47] and to continuously review and update privacy measures.[48] Accountability requirements permeate the Regulation. For example, under Article 28, where a controller employs third-party processors, it is required to hold the processors accountable through mandatory contract terms.[49]

Another significant accountability mechanism in the GDPR is the requirement to conduct data protection impact assessments, originally referred to as privacy impact assessments (PIAs) under US law, for high risk processing activities.[50] PIAs have their origins in guidelines issued by the US Department of Health, Education and Wellness in 1973.[51] Since then, they have been adopted in guidance issued by privacy commissioners from Australia, Canada,

47. *Id.* art 30(1).

> Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information: (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; (b) the purposes of the processing; (c) a description of the categories of data subjects and of the categories of personal data; (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards; (f) where possible, the envisaged time limits for erasure of the different categories of data; (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1). *Id.*

48. *Id.* art 24(1).

> Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary. *Id.*

49. *Id.* art 28.

50. *Id.* art 35(1).

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks. *Id.*

51. *See* U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973) [hereinafter HEW REPORT], https://www.justice.gov/opcl/docs/rec-com-rights.pdf [https://perma.cc/Y4GR-27M8].

Hong Kong and New Zealand in the mid-1990s.[52] In the GDPR, the PIA requirement is part of a broader mandate that includes appointing a Data Protection Officer to promote privacy governance within organizations that engage in risky processing.[53] These efforts build off the experiences of privacy management programs among US companies and appear aimed at narrowing the gap between privacy protections on the books and on the ground.[54]

III. THE DATA PROTECTION OFFICER

Since 1977, German law has required public authorities and companies of a certain size to appoint data protection officers (DPOs).[55] These officers were tasked with supervising compliance with data protection laws and reporting to management, but they did not have responsibility for implementing data protection programs.[56] Building off the German experience, the Directive sought to encourage the use of DPOs to ensure compliance. Article 18 exempted a controller from the requirement to notify a supervisory authority of its processing activities if it appointed a DPO.[57] However, the scope of the DPO's role was narrow: to avoid the reporting requirements, the DPO was required to ensure "in an independent manner the internal application of the national provisions," and keep a "register of processing operations carried out by the controller."[58]

Although the concept of an internal data protection function developed first in the EU, it has risen to prominence as a central feature under the US approach to privacy protection. In the US, the role of the Chief Privacy Officer (CPO) first appeared in the 1990s, when companies created internal positions for privacy specialists.[59]

---

52. *See generally* David Tancock et al., The Emergence of Privacy Impact Assessments (May 2010) (unpublished manuscript), http://www.hpl.hp.com/techreports/2010/HPL-2010-63.pdf [https://perma.cc/UEA2-3A82].

53. GDPR, *supra* note 1, art 37(1).

> The controller and the processor shall designate a data protection officer in any case where: (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10. *Id.*

54. *See generally* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

55. Gesetz zum Schutz vor Miebrauch personenbezogener Daten bei der Datenverarbeitung [BDSG] [Federal Data Protection Act], Jan. 27, 1977, BGBL I at 201, Jan. 14, 2003, BGBL I at 66, as amended by Gesetz, Aug. 22, 2006, BGBL I at 1970.

56. *Id.* § 7.

57. Data Protection Directive, *supra* note 11, art. 18(2).

58. *Id.*

59. Clearwater & Hughes, *supra* note 40, at 904–07.

Unlike the German DPOs, who were typically low to mid-level managers, the US based CPOs often are executives and C-level officers, reflecting a perception within these firms of data as a strategic asset and privacy as a core function inherent in establishing consumer trust and brand reputation. While their responsibilities vary from firm to firm, most CPOs are responsible for implementing privacy management programs that include conducting PIAs, auditing company practices, managing data flows and training employees, in addition to monitoring compliance. Increasingly, CPOs are involved in product design and engineering processes. By 2015, according to a joint study by the IAPP and EY, US companies, on average, had larger privacy budgets and greater staff resources than their European counterparts.[60]

The DPO role outlined in the GDPR takes elements from both the EU and US models. Like under German law, DPOs are mandatory for public authorities and for a subset of companies—those that process sensitive data on a large scale or that conduct "regular and systematic monitoring of data subjects on a large scale."[61] But, like the US CPO, the DPO's role will extend beyond monitoring compliance and record-keeping to include strategic planning, employee training, auditing, advising on PIAs, and interacting with supervisory authorities.[62] With GDPR, EU based DPOs will potentially elevate to a level commensurate with their US counterparts.

IV. DATA BREACH NOTIFICATION

In 2002, California enacted the world's first data breach notification law.[63] The law required a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person.[64] For breaches involving more than 500 California residents, organizations were also required to notify the state's Attorney General.[65]

The novel California law had a profound impact on the development of privacy laws and policies in the US. As data breaches came to light, consumers, regulators, the media and corporate boards were exposed to the universe of risks posed by hacking, negligence and rogue employees. Waves of class action lawsuits and a constant drumbeat of front-page news reports have

60. IAPP-EY ANNUAL PRIVACY GOVERNANCE REPORT 2015, at 95 (2015), https://iapp.org/media/pdf/resource_center/IAPP-EY_Privacy_Governance_Report_2015.pdf [https://perma.cc/YGA3-S6NW].

61. GDPR, *supra* note 1, art 37(1)(b).

62. *Id.* art. 39.

63. Cal. Civ. Code §§ 1798.29, 1798.82, 1798.84 (West 2019).

64. *Id.* §§ 1798.29, 1798.82.

65. *Id.* §§ 1798.29(e), 1798.82(f).

placed these privacy risks at the forefront of consumer consciousness and highlighted the strategic importance of privacy protection for firms that hold personal data.[66]

The success of California's data breach law is manifest in that all 50 states and the District of Columbia followed the state's lead and enacted their own data breach notification laws.[67] These laws encode an assortment of standards around who must comply, what constitutes a breach, what qualifies as personal information, who must be notified, and what needs to be included in the notice. As a result, virtually every organization that handles the personal data of US residents must invest significant resources in privacy management or risk damaging disclosures to consumers in case of a breach.

The US model of breach notification was so successful that it has been replicated around the world.[68] In 2009, the EU introduced breach notification for electronic communications service providers in the amendments to the E-Privacy Directive.[69] Under the GDPR, breach notification will extend to all controllers of personal data. Controllers must notify a competent supervisory authority "not later than 72 hours after . . . becom[ing] aware of [a breach]," unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons."[70] Where a breach "is likely to result in a high risk [for data subjects]," the GDPR requires notification to affected individuals "without undue delay."[71] In this arena too, EU law adopts and implements US born privacy measures.

V. PRIVACY BY DESIGN

Related to the principle of accountability is the idea that organizations should incorporate privacy into a product or service from its moment of inception, rather than as an after the fact compliance task. In the 1990s, Ann Cavoukian, then-Privacy Commissioner of Ontario, was the first to formally introduce the notion of "Privacy by Design."[72] It offers a vision for networked data systems whereby privacy is engineered into the architecture of a

66. *See* Michelle Kisloff, *Data Class Actions in the US*, HOGAN LOVELLS (Aug. 16, 2018), https://www.hlmediacomms.com/2018/08/16/data-class-actions-in-the-us/ [https://perma.cc/2UZ5-S7K7].

67. Security Breach Notification Laws, NAT'L CONF. ST. LEGISLATURES (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx [https://perma.cc/53YC-E3X8].

68. *See generally* WORLD LAW GRP., GLOBAL GUIDE TO DATA BREACH NOTIFICATIONS (2d ed. 2016), http://www.theworldlawgroup.com/Document.asp?DocID=115509 [https://perma.cc/YT95-UW2L].

69. Council Directive 2009/136/EC, 2009 O.J. (L 337) 11.

70. GDPR, *supra* note 1, art. 33(1).

71. *Id.* art. 34(1).

72. ANN CAVOUKIAN, PRIVACY BY DESIGN: 7 FOUNDATIONAL PRINCIPLES (2011), https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf [https://perma.cc/KA35-V9ZU].

product and expressed throughout its lifecycle. For products that offer users multiple choices of settings, the most privacy protective setting should be the default. Privacy by design first gained significant regulatory traction in the US, where it was a central tenet of the FTC's 2012 framework.[73]

The GDPR incorporates privacy by design in Article 25. Controllers must implement appropriate measures "both at the time of the determination of the means of processing and at the time of the processing itself" to safeguard personal data consistent with the Regulation.[74] These measures should include data minimization and pseudonymization—collecting only the information required for the activity and taking steps to reduce the identifiability of data sets. Additionally, under Article 25(2), controllers must provide privacy protective settings "by default" relating to how data are processed, how long they are stored, and to whom they are accessible.[75]

VI. PROTECTIONS FOR CHILDREN

In 1997, the FTC investigated a website directed at children called KidsCom. The result of the investigation, which found that KidsCom's practices of collecting personal information from children "likely were deceptive or unfair in violation of Section 5 of the FTC Act," served as the catalyst for Congress's decision to protect children's privacy online.[76] In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA).[77] The first privacy act in the world specifically directed at protecting children's information, COPPA introduced responsibilities for websites that knowingly collect the personal information of children under the age of 13.

---

73. FTC REPORT, *supra* note 10, at 22–34.

74. GDPR, *supra* note 1, art. 25(1).

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. *Id.*

75. *Id.* art. 25(2).

76. Press Release, Toby Levin, Bureau of Consumer Prot., Fed. Trade Comm'n, FTC Staff Sets Forth Principles for Online Information Collection from Children (July 16, 1997), https://www.ftc.gov/news-events/press-releases/1997/07/ftc-staff-sets-forth-principles-online-information-collection [https://perma.cc/CL6Y-8QVR].

77. 15 U.S.C. §§ 6501–6506 (2018).

In the EU, including under the Directive, there were no special protections for children's data. Of course, protections for children could be inferred from the Directive, but none were explicit.[78] The GDPR, by contrast, draws from the US experience to provide express protections for children. Like COPPA, the GDPR requires controllers to collect parental consent for children below the age of 13 (although the statutory default age is 16, Member States are provided leeway to reduce that age to 13). Specifically, the GDPR creates special protections around marketing to children and creating user profiles,[79] ensuring proper notice to children of data practices,[80] and assuring that children have the "right to be forgotten" when they consented to processing without fully understanding the risks.[81] These protections apply only to "information society services,"[82] which mirrors COPPA's application to "online services."[83]

CONCLUSION

As the EU and US remain locked in a high-profile impasse over national security access to personal data, this article demonstrates that below a superficial crust of resentment and discord, the two blocks share fundamental values and approaches to privacy regulation. After all, before there was discord, there was a long history of cooperation and co-equal development. Indeed, the very concept of information privacy was conceived by the American scholar, Alan Westin, whose seminal work, *Privacy and Freedom*,[84]

78. Article 29 Data Protection Working Party, *Opinion 2/2009 on the Protection of Children's Personal Data*, at 9, 398/09/EN, WP 160 (Feb. 11, 2009).

79. GDPR, *supra* note 1, pmbl. 38.

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child. *Id.*

80. *Id.* pmbl. 58 ("Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.").

81. *Id.* pmbl. 65.

> That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. *Id.*

82. *Id.* art. 8.

83. 15 U.S.C. §§ 6502(a)(1) (2012) ("It is unlawful for an operator of a website or online service directed to children. . . .").

84. ALAN F. WESTIN, PRIVACY AND FREEDOM (1st ed. 1967).

laid the foundation for the first ever articulation of the FIPPs in a committee report to the US Department of Health Education and Welfare in 1973.[85] European national law through the 1970s and the US Privacy Act of 1974 took up the mantle, adopting a variety of approaches to privacy regulation. The 1980 OECD Guidelines coalesced around the FIPPs, which would again find expression in the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 1981.[86]

By 1995, as the EU moved toward the omnibus approach of the Directive, the US opted for a limited, sectoral intervention. But that does not mean that the development of privacy protections halted. To the contrary, an entire industry was born devoted to implementing organizational accountability and minimizing privacy risks for the protection of brand reputations and consumer trust. The GDPR—as much as it is true to the European form—adopts many of the innovations that grew out of American legal traditions and experience. From respecting the reasonable expectations of consumers to implementing accountability and promoting the profession of privacy, the GDPR reflects an emergent global consensus, as organizations everywhere seek to operationalize privacy in an interconnected digital world. Far from escalating the conflict, the GDPR may signal the start of a transatlantic privacy convergence.

85. HEW REPORT, *supra* note 51.

86. Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, ETS 108.