JOURNAL OF INTERNATIONAL ACCOUNTING RESEARCH
Vol. XX, No. XX
MONTH YEAR
pp. 1–15

American Accounting Association
DOI: 10.2308/JIAR-2025-039

COMMENTARY

Global Data Protection Regulation: Implications for Accounting Research and Practice

Jayanthi Krishnan
Temple University

Steven A. Maex
George Mason University

ABSTRACT: This commentary explores the implications of global personal data protection regulations for accounting researchers and practitioners. At the 2025 American Accounting Association (AAA) International Accounting Section Midyear Meeting, a panel discussion was held on global technology trends impacting accounting with one of the topics being the trend toward increasing legislative protections over data privacy in the wake of the European Union's General Data Protection Regulation. The expansion of these laws across global jurisdictions, spurred by advancements in digital technologies (e.g., social media, artificial intelligence) and concerns over personal data handling by organizations, presents important opportunities for accountants, whose role has increasingly evolved toward broader responsibilities in information assurance. This article summarizes (and expands upon) some of the key points of the presentation relating to data privacy at the 2025 panel and offers suggestions for how both researchers and practitioners can contribute to and benefit from this evolving regulatory paradigm.

JEL Classifications: M41; M48; K24.

Keywords: data privacy; cybersecurity; SOC reporting; general data protection regulation.

I. INTRODUCTION

In an era defined by rapid global digital transformation, personal data privacy has become "one of the most important issues of the 21st century" (Tim Cook, Apple CEO, as cited in Gilchrist 2018). Spurred in recent years by increased reliance on cloud services and artificial intelligence (AI)-driven analytics, the volume and sensitivity of personal data being processed and utilized continues to grow exponentially. This trend has coincided with a growing skepticism among individuals about how firms handle their personal data (McClain, Faverio, Anderson, and Park 2023). In this environment, governments have worked to enact data protection laws intended to provide individuals with greater control over their personal data. These laws require companies to strengthen core information governance and cybersecurity processes, and they influence the information organizations disclose to the market (e.g., when obtaining consent for data collection or reporting cybersecurity incidents). Although these regulations are often considered

We appreciate the feedback from fellow panelists, Asher Curtis and Emmanuel De George, as well as other conference attendees. We also appreciate the helpful comments of Ling Lei Lisic (editor), an anonymous reviewer, Jagan Krishnan, Jess Filosa, and Stefan Slavov. The authors have no conflicts of interest related to this research.

This commentary discusses one subtopic of a panel entitled "Accounting in a Digital World" at the 2025 American Accounting Association (AAA) International Accounting Section Midyear Meeting.

Jayanthi Krishnan, Temple University, Fox School of Business, Department of Accounting, Philadelphia, PA, USA; Steven A. Maex, George Mason University, Costello College of Business, Accounting Area, Fairfax, VA, USA.

Any use of generative artificial intelligence (AI) or AI tools by the author(s) has been disclosed in the "Declaration of Generative AI and AI-Assisted Technologies" section.

Editor's note: Accepted by Senior Editor Ling Lei Lisic.

Submitted: August 2025
Accepted: November 2025
Early Access: December 2025

within the domains of law and information technology (IT), they have traditionally received less attention in the field of accounting. Nevertheless, we posit that privacy laws are highly relevant to both accounting practitioners—who possess the skills needed to help organizations manage key information assets—and accounting researchers—who study the impact of information revealed to the marketplace and the associated changes in governance and operational processes. The goal of this paper is to (1) present an overview of the evolving regulatory landscape regarding personal data protection and (2) discuss the implications of these regulations as well as the opportunities they provide accounting practitioners and researchers.

Data protection is broadly defined as "the practice of safeguarding sensitive information from data loss and corruption" (IBM 2025). Although the concept can apply to any critical information asset managed or used by an organization, its use in regulatory contexts almost exclusively refers to the protection of personal information in support of individuals' fundamental data privacy rights. These rights aim to ensure transparency, accountability, and individual autonomy in the handling of personal data, empowering individuals to control how their personal information is collected, used, and shared. Common protections include the right to access one's data, understand how it is processed, correct inaccuracies, and request deletion (i.e., the "right to be forgotten"). These rights form the foundation of data protection regulations, which have evolved significantly since the United Nations General Assembly first recognized the right to legal protection against "arbitrary interference with [individuals'] privacy" (United Nations 1948, Article 12).

As of 2025, over 160 countries have some form of national data privacy regulation, up from fewer than 100 in 2013 (DLA Piper 2025; Greenleaf 2013, 2025).[1] The landmark regulatory shift that spurred many of these new laws was the European Union's General Data Protection Regulation (GDPR), adopted in 2016 and enforced beginning in 2018. As noted by the Brookings Institution, the GDPR "changed the privacy dialogue for businesses and governments around the world" (Chin-Rothmann 2019). Since then, numerous regulations modeled after the GDPR have emerged in major global markets, including China, India, and Brazil, as well as in U.S. states, such as California.

Although privacy regulation has traditionally been the focus of disciplines outside of accounting (e.g., law and information technology), there is a growing recognition that accounting practitioners can play a vital role in helping firms respond to privacy expectations from individuals, particularly when codified into regulation. By broadening the accountant's role to encompass information assurance more generally (i.e., extending beyond traditional financial reporting), accounting practitioners can contribute meaningfully to the design, evaluation, and oversight of systems that ensure the confidentiality, integrity, and availability (CIA) of personal data. Likewise, accounting scholars have begun to evaluate the implications of these privacy regulations for firms and financial markets. As these laws continue to proliferate, numerous opportunities arise for accounting researchers to understand their implications for the world of accounting and assurance.

The remainder of the paper proceeds as follows. Section II provides a conceptual overview of data privacy, data protection, and cybersecurity as well as the application of these terms to data protection regulation. Section III provides an overview of the global regulatory landscape in relation to data protection. Sections IV and V discuss implications of this evolving regulatory environment for accounting practitioners and researchers, respectively. Section VI concludes.

II. CONCEPTUAL OVERVIEW

Three interrelated concepts—data privacy, data protection, and cybersecurity—underpin the global regulatory landscape for personal data. Data (or information) privacy refers to the right of individuals "to have some control over how your personal information is collected and used" (IAPP 2025, paragraph 1).[2] Chapter 3 of the GDPR, for example, outlines eight specific rights of individuals including the right to be informed regarding the personal data that is collected, the right to rectify personal data that is incorrect, and the right to request the erasure of personal data.[3] Hence, data privacy sets the ethical and legal boundaries for data collection, retention, and use.

Data protection refers to measures adopted by organizations to support data privacy rights. These comprise organizational and technical measures. Organizational measures delineate the roles, policies, and processes that allow firms to identify and properly handle personal data held and processed by the organization. These include the implementation of internal privacy and data handling policies, external notices and communications to customers, assessments of data privacy implications when implementing new systems or sharing data with third parties, and processes to identify and respond to personal data breaches.

[1] For a comprehensive overview of privacy regulations globally, see Greenleaf (2023).
[2] As a technical matter, *data* refers to raw elements (e.g., a person's national identification number (ID number)), whereas *information* refers to data that have been organized or contextualized to convey meaning (e.g., triangulating an individual's location using their purchase history). As this distinction is not critical for our purposes, we use these terms interchangeably throughout the paper.
[3] The full regulatory text of the GDPR is available here: https://gdpr-info.eu/

These organizational measures in turn dictate the technical measures (i.e., tools, technologies, and systems) that the organization may employ to help ensure the security (i.e., confidentiality, integrity, and availability—known as the "CIA triad") of personal data and achieve compliance with applicable data protection regulations. These measures can be a combination of preventive (e.g., encryption and pseudonymization technologies, firewall and network perimeter management, and access controls) and detective (e.g., audit and monitoring tools to track when data has been accessed) security controls over personal data and the systems housing it. Backup and recovery processes that maintain personal data in a secure format are also critical technical measures.

Finally, although data privacy and data protection focus on the rights of individuals and the policies and practices organizations adopt to manage personal data responsibly, cybersecurity serves as the backbone that enables these protections. Cybersecurity encompasses the tools, strategies, and protocols used to defend systems and data from unauthorized access, attacks, and disruptions. This set of tools and protocols includes critical areas such as intrusion detection, threat monitoring, incident response, and vulnerability management, and is a foundational enabler of both data protection and, by extension, data privacy.

III. GLOBAL DATA PROTECTION REGULATION LANDSCAPE

Data Protection Regulation

The Right to Privacy in the Pre-Computerized Environment (Pre-1970)

The right to privacy has evolved over centuries, shaped by legal, philosophical, and technological developments. Its conceptual foundations are often linked to liberal Enlightenment thought, particularly John Locke's ideas on individual autonomy and property (Locke 1988, 1689). However, it was not until the late 19th century that privacy began to emerge as a distinct legal concept. A pivotal moment came in 1890 with Samuel Warren and Louis Brandeis's seminal *Harvard Law Review* article, "The right to privacy," which argued for a "right to be let alone" in response to growing concerns over invasive journalism and new technologies like photography (Warren and Brandeis 1890). This concept gradually entered constitutional and legal frameworks in various countries. Globally, privacy was enshrined as a human right by the United Nations General Assembly in Article 12 of the *Universal Declaration of Human Rights* in 1948 and later in Article 17 of the *International Covenant on Civil and Political Rights* in 1966 (United Nations 1948, 1966).

Data Privacy in the Computerized Environment (1970s to 2000s)

The foundation of today's global data protection landscape lies in the recognition of privacy as a fundamental human right, a concern that gained urgency with the rapid expansion of computerized data processing in the mid-20th century. One of the earliest milestones was Sweden's 1973 Data Act, widely regarded as the world's first national law to regulate the automated processing of personal data (Freese 1977). Alongside this legislative landmark in Europe, a 1973 report issued by a special committee to the U.S. Department of Health, Education, and Welfare established "a set of fundamental principles for fair information practice" (Hartzog and Richards 2020). These Fair Information Practice Principles (FIPPs) included many of the key foundational elements that form the basis for modern data protection regulations including the need for notice and consent prior to collecting personal data and the responsibility of organizations to properly secure and prevent misuse of such data (United States Department of Health, Education, and Welfare (US DHEW) 1973).[4]

Informed by these FIPPs, the Organisation for Economic Co-operation and Development (OECD) published its influential "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" in 1980 (OECD 2002). These principles, listed and summarized below, formed the basis for privacy regulations that followed:

1. **Collection Limitation:** Personal data should be obtained lawfully and fairly, with knowledge or consent of the data subject, and limited to what is necessary.
2. **Data Quality:** Personal data should be relevant to its intended purpose and accurate, complete, and kept up to date for its purpose.
3. **Purpose Specification:** The purposes for collecting personal data should be specified at the time of collection, and any later use must be compatible with those purposes.
4. **Use Limitation:** Personal data should only be used or disclosed for the stated purposes, unless the individual consents or the use is authorized by law.

[4] Within the United States, these FIPPs were codified into law in the U.S. Privacy Act of 1974. This act continues to form the basis for the regulation of the collection, use, and disclosure of personal information by federal government agencies to this day (United States Office of Privacy and Civil Liberties (US OPCL) 2022).

5. **Security Safeguards:** Reasonable security measures must protect personal data against risks such as loss, unauthorized access, or misuse.
6. **Openness:** Organizations should be transparent about their personal data practices and provide clear information about data holdings and use.
7. **Individual Participation:** Individuals should be able to access, correct, or challenge their personal data and understand how and why it is used.
8. **Accountability:** Data controllers are responsible for complying with these principles and must demonstrate adherence to them.

Following the establishment of these principles, the European Union took a leading role in formalizing data protection with its 1995 Data Protection Directive (DPD), which sought to harmonize privacy laws across member states and introduced the concept of personal data rights on a large scale. Although this directive was a sizeable leap forward for privacy regulation globally, the years that followed brought technological evolutions (e.g., social media) that changed the ways in which personal information was shared and used by corporations. Further, although the DPD provided a common framework for personal data protection, it relied on individual member states to translate the directive into national laws, resulting in fragmented and inconsistent implementation across the EU. By the early 2010s, there was recognition in the European Union that such regulations would need to be modernized and more consistently applied across member states.

The Birth of Modern Privacy Regulation (2010s and 2020s)

The GDPR was adopted by the European Union in 2016 and became enforceable in 2018. When taking effect, the regulation "positioned the European Union as the world's privacy champion," setting a new global benchmark for data protection (Chander, Kaminski, and McGeveran 2021, 1734). In addition to establishing greater uniformity across member states in comparison to the DPD, the GDPR also introduced the concept of extraterritoriality meaning that it applied to any organizations across the globe that handle the personal data of individuals in the EU. It also expanded the scope of rights protected, including the rights of data portability[5] and the right to be forgotten, shortened the period allowable to notify authorities in the case of a data breach (to within 72 hours), and increased the size of fines (to up to €20 million or up to 4 percent of total worldwide annual turnover, whichever is higher) for violations of the regulation.

Since the passage of the regulation, over 2,600 fines have been levied at a total cost of over €6.7 billion across EU countries (as of October 2025; GDPR Enforcement Tracker 2025). Over €4 billion of these fines have been levied by Ireland's Data Protection Commission, reflecting its role as the lead supervisory authority for many global technology firms (e.g., Meta, Google, Apple) that maintain their EU headquarters there. In contrast, Spain's Data Protection Authority (i.e., the Agencia Española de Protección de Datos—AEPD) has been the most active in terms of enforcement volume, issuing nearly 1,000 fines to date. The most common alleged infringements of the regulation include not having a sufficient legal basis for data processing, not complying with general data processing principles, and not having sufficient technical and organizational measures to ensure information security.[6]

Subsequent to passage of the GDPR, numerous national legislatures have enacted new or amended existing regulations based on similar principles to the GDPR. These include Brazil's General Data Protection Law, China's Personal Information Protection Law, South Africa's Protection of Personal Information Act, Japan's Act on the Protection of Personal Information, and India's Digital Personal Data Protection Act. See Table 1 for an overview of the key features of each of the above regulations. In addition to defining the protected privacy rights, each specifies penalties for infringement, thus creating monetary incentives for compliance. Overall, as of 2025, over 160 countries have enacted some form of national data privacy regulation and the pace of growth in the rollout and evolution of these regulations does not appear to be slowing (DLA Piper 2025). Asia, particularly, has seen a rapid evolution in its data protection landscape with India, Indonesia, and Saudi Arabia all enacting or enforcing new data protection laws since the start of

[5] As outlined in GDPR Article 20, this is the right to take personal data provided by the data subject to one controller and move it to another controller without hindrance. This right, for example, allows individuals to export photos, videos, and posts from one social media platform to another in a structured, machine-readable way.

[6] For example, in 2022, the French privacy regulator (Commission Nationale de l'Informatique et des Libertés (CNIL)) fined both Google and Facebook significant sums (€150 million and €60 million, respectively) for making website tracking cookies hard to refuse. Due to this lack of transparency and fairness with regards to data processing, both entities were deemed to have had an insufficient legal basis for processing personal data via these cookies (Milmo 2022). Likewise, in 2020, Marriott International was fined £18.4 million by the United Kingdom's Information Commissioner's Office for failing to adequately secure customer data during the acquisition of Starwood Hotels and Resorts Worldwide. This fine followed a breach of 339 million guest records, of which 7 million related to individuals in the U.K., highlighting the extraterritorial reach of the regulation to a U.S.-headquartered company (Page 2020).

TABLE 1

Overview of Prominent Personal Data Protection Regulations

Regulation[a]	Impacted Organizations	Scope of Protected Data	Potential Fines
General Data Protection Regulation Jurisdiction: European Union Effective: 2018	EU-based organizations processing personal data as well as non-EU organizations offering goods/services or monitoring behavior of individuals in the EU. (Art. 3)	Any information related to an identified or identifiable natural person, including identifiers (e.g., name, IP address), locations, etc. (Art. 4(1))	Up to greater of €20 million or 4% of annual worldwide turnover of the preceding financial year. (Art. 83)
California Consumer Privacy Act/ California Privacy Rights Act Jurisdiction: California (U.S.) Effective: 2020/Amended: 2023	Any for-profit business that collects personal information of California residents, determines the purposes and means of processing that information, does business in California, and meets thresholds related to gross revenue or personal data collected. (California Civ Code § 1798.140)	Defined broadly as any information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. (California Civ Code § 1798.140)	$2,500 per violation or $7,500 per intentional violation (adjusted biennially for inflation). (California Civ Code § 1798.155)
General Data Protection Law Jurisdiction: Brazil Effective: 2020	Any organization, domestic or foreign, that processes personal data within Brazil, targets individuals in Brazil with goods or services, or processes data collected from individuals located in Brazil. (Art. 3)	Any information related to an identified or identifiable natural person. (Art. 5)	Up to 2% of the organization's revenue in Brazil from the previous fiscal year capped at 50 million Brazilian real (~$9M USD) per violation. (Art. 52)
Personal Information Protection Law Jurisdiction: China Effective: 2021	Any entity processing personal data of individuals in China, including foreign firms. (Art. 3)	Personal information identifying a person directly or indirectly, including name, ID number, biometric, address, etc. (Art. 4)	Up to 50 million Chinese Yuan or 5% of revenue; serious violations can lead to business shutdown. (Art. 66)
Protection of Personal Information Act Jurisdiction: South Africa Effective: 2021	Public or private bodies domiciled in South Africa, or foreign entities using processing means in South Africa (unless merely forwarding data). (Sections 1–3)	Any information about an identifiable, living, natural person. (Section 1)	Administrative fine up to 10 million South African Rand (~$500,000 USD). (Section 109)
Act on the Protection of Personal Information Jurisdiction: Japan Effective: 2003 (Initial) / 2022 (Amended)	Businesses handling personal information databases including foreign entities offering goods/services to Japan. (Art. 171)	Personal info identifying a specific individual and associated identification codes. (Art. 2(1))	Up to 100 million Japanese Yen for corporations. (Art. 184)

(continued on next page)

TABLE 1 (continued)

Regulation[a]	Impacted Organizations	Scope of Protected Data	Potential Fines
Digital Personal Data Protection Act Jurisdiction: India Effective: 2023	Applies to all entities processing digital personal data in India, and to foreign entities processing data in connection with offering goods/services to Indian citizens. (Section 3)	Any data about an individual who is identifiable by or in relation to such data. (Section 2(t))	Up to 250 crore Indian Rupees (~$30M USD) per instance of noncompliance. (Section 33)

[a] Full regulatory texts available as follows: General Data Protection Regulation (EU): https://gdpr-info.eu/; California Privacy Rights Act: https://thecpra.org/; General Data Protection Law (Brazil): https://lgpd-brazil.info/; Personal Information Protection Law (China): http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm; Protection of Personal Information Act (South Africa): https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf; Act on the Protection of Personal Information (Japan): https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en; Digital Personal Data Protection Act (India): https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9-f04e6fb4f8fef35e82c42aa5.pdf

2023. Although the United States has yet to adopt a comprehensive national data protection law akin to the GDPR, several states have enacted similar legislation, most notably California's Consumer Privacy Act (CCPA).[7]

Related Regulatory Focus

Data Breaches

Although data protection regulations like the GDPR establish comprehensive rules for the collection, processing, and safeguarding of personal data, a related but distinct regulatory domain in some jurisdictions governs how organizations must respond to the most salient of data privacy issues, personal data breaches. In the United States, for example, state-level breach notification laws have been in place since the early 2000s. These laws, which mandate that organizations inform affected individuals when their personal information has been compromised, typically reside under consumer protection statutes rather than broader privacy or disclosure frameworks.[8] These laws differ significantly across states in terms of scope, timing, and enforcement, creating a fragmented legal landscape that firms must navigate in parallel with broader data privacy obligations.

Cybersecurity Risk

Coinciding with the global trend toward stricter data protection regulation is a growing interest among stakeholders in the cybersecurity risks faced by firms. This heightened concern has drawn the attention of financial market regulators, who have responded by expanding disclosure requirements for public companies regarding material cybersecurity threats and incidents. The U.S. Securities and Exchange Commission (SEC) has played a leading role in this area. In 2011, the SEC issued nonbinding guidance on the disclosure of material cyber risks, which amplified the importance of cybersecurity in corporate reporting and led to a marked increase in related disclosures—particularly in Item 1A (Risk Factors) of firms' 10-K filings (SEC 2011).[9] More recently, in 2023, the SEC released new rules to expand disclosure requirements for firms in areas such as cybersecurity risk management practices, governance structures, and incident reporting procedures (SEC 2023). These requirements are intended to benefit investors by ensuring that cybersecurity disclosures are made in "a more consistent, comparable, and decision-useful way" (SEC 2023). Over time, the risk factor disclosures encouraged by these SEC pronouncements have increasingly discussed global data privacy regulations. In Appendix A, we provide examples of such risk factor disclosures.

Other jurisdictions have expressed or implied similar expectations regarding cybersecurity risk disclosure. For example, although the U.K.'s Financial Reporting Council (FRC) makes no explicit mention of cybersecurity in its recently released 2024 Corporate Governance Code, a study by the U.K. Department for Science, Innovation, and Technology (DSIT) found that many large U.K. firms disclose cybersecurity risks in the "Principal Risks" section of their annual reports, as part of broad governance and risk management obligations under the Companies Act 2006 and the U.K. Corporate Governance Code (Department for Science, Innovation, and Technology (DSIT) 2025).[10]

Globally, these disclosure-based regulations complement laws in many jurisdictions that require organizations in "critical" industries to design and implement cybersecurity controls. These include, for example, Australia's Security of Critical Infrastructure Act, Singapore's Cybersecurity Act, and Japan's Basic Act on Cybersecurity. These laws typically focus on topics such as risk management, incident reporting, and executive accountability and target critical sectors such as energy, utilities, and financial services. The rollout of the EU's Network and Information Systems Directive 2 (NIS2 Directive) starting in 2024 exemplifies the expansion of such regulations to other sectors (e.g., waste management, food, manufacturing, public administration) as well (European Commission 2025).

[7] As of July 2025, 19 of the 50 U.S. states have implemented laws modeled, to some extent, after the GDPR imposing additional requirements on personal data processing. For a comprehensive overview of privacy regulation at the state-level in the U.S., see the U.S. State Privacy Legislation Tracker available here: https://iapp.org/resources/article/us-state-privacy-legislation-tracker/. Outside of these state-level laws, national privacy laws in the United States have historically been more industry-specific (e.g., the Health Insurance Portability and Accountability Act for health information, the Gramm-Leach-Bliley Act for financial information), reflecting the country's sectoral approach to privacy rather than a unified, comprehensive framework like the GDPR.

[8] For a summary of these laws and a catalogue of the applicable statutes within each U.S. state, see the National Conference of State Legislatures' Summary of Security Breach Notification Laws available here: https://www.ncsl.org/technology-and-communication/security-breach-notification-laws

[9] Numerous studies have explored in depth the risk factor disclosures that emerged following the SEC's disclosure guidance (e.g., Li, No, and Wang 2018; Cheong, Yoon, Cho, and No 2021; Chen, Henry, and Jiang 2023; and Florackis, Louca, Michaely, and Weber 2023).

[10] The recently released 2024 U.K. Corporate Governance Code includes new guidance that speaks to the role of the board in "strategically approaching cyber security, ensuring operational resilience and continuous functioning of the business" (Financial Reporting Council (FRC) 2024). Further, provision 29 of the Code requires that the board carry out an annual review of the effectiveness of the company's risk management and internal control framework, which includes "all material controls," even those that are not related directly to financial reporting (e.g., cybersecurity controls).

Artificial Intelligence

Lastly, any discussion of data privacy regulation in the current environment must also consider its intersection with the rapid expansion of AI. Because AI models are typically trained on large datasets often containing personal or sensitive information, data privacy requirements are an important constraint to ensure that AI models are developed in a manner that "respects human rights and democratic values" (OECD 2025). As a result, many jurisdictions are designing AI regulations that build upon and reinforce existing privacy frameworks. For example, the EU AI Act creates legal requirements for "high-risk" applications (e.g., automated evaluation of job applicants) and even bans certain use cases such as government-managed social scoring (EU AI Act 2025). Looking ahead, a central regulatory challenge will be ensuring that emerging AI-specific rules complement, rather than conflict with, established data protection regimes.

IV. IMPLICATIONS FOR ACCOUNTING PRACTITIONERS

Accountants possess deep expertise in evaluating risks and assessing internal controls, particularly in relation to one of the most heavily regulated classes of information globally—that related to financial reporting. This foundational experience positions them to contribute meaningfully as organizations confront expanding regulatory and stakeholder expectations related to personal data. At their core, data protection laws require firms to demonstrate accountability, transparency, and effective risk management over personal information. The accountant's foundational skillset, rooted in risk assessment, control testing, and assurance, can be readily applied to this new domain if augmented with appropriate legal and technical knowledge on the topic. Accountants can support organizations internally by defining and implementing data governance processes or externally by providing assurance to outside stakeholders. This latter opportunity echoes themes presented in Knechel (2021), which outlines ways in which the auditing profession can reclaim its economic imperative by expanding coverage to cybersecurity-related areas.

An important response by the accounting profession to growing concerns over data governance and cybersecurity is the American Institute of Certified Public Accountants (AICPA)'s increased emphasis on System and Organization Controls (SOC) reporting services. Most well known for SOC 1 reports—relating to internal controls over financial reporting (ICFR) at service organizations—the SOC framework has expanded to include assurance services over the AICPA's Trust Services Criteria (TSC).[11] Within the TSC framework, five key categories are used to evaluate an organization's controls: security, availability, processing integrity, confidentiality, and privacy. SOC 2 and SOC 3 reports, which are based on this framework, enable organizations that process data on behalf of clients (e.g., cloud service providers, payroll processors, data hosting platforms) to demonstrate their commitment to robust data governance, cybersecurity, and risk management practices.[12] These reports provide service organizations' customers independent assurance that their service providers have effective controls in place to protect sensitive data and support compliance with relevant legal, regulatory, and contractual obligations. This assurance is increasingly important in a digital economy where nearly 95 percent of global organizations leverage cloud services (Flexera 2019). Concurrently, data privacy (and related) regulatory pressures have further accelerated the demand for these SOC 2 and SOC 3 reports (AICPA 2023; KPMG UK 2024).

The growth in demand for these services highlights the increasing need for accountants to develop skills in areas related to data protection, such as IT controls, data governance, and cybersecurity.[13] Cognizant of this need, accounting credentialing organizations around the world have expanded the knowledge base tested on their certification exams to include the above areas. For example, in 2024 the AICPA transformed the Certified Public Accountant licensure model (i.e., "CPA Evolution") to emphasize the role of technology in accounting. The new format introduces new technology topics on each core exam (i.e., Auditing and Attestation (AUD), Financial Accounting and Reporting (FAR), and Taxation and Regulation (REG)) and offers a standalone discipline exam focused on information systems and controls (one of three discipline choices) that CPA aspirants can select as their fourth and final exam (AICPA 2025). The knowledge base for this "ISC" discipline explicitly includes topics related to data privacy and data protection

[11] The suite of SOC services is governed under the AICPA's attestation standards (AT-C sections), which provide the overarching framework for attestation engagements. Specifically, SOC 1 reports are conducted under AT-C Section 320, whereas SOC 2 and SOC 3 reports are conducted under AT-C Section 205, based on the Trust Services Criteria. More information on the entire suite of SOC service offerings is available here: https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

[12] Although the underlying examination performed by the service auditor to arrive at SOC 2 and SOC 3 reports is the same, the key difference between the two reports lies in the level of detail presented. SOC 2 reports are intended for a restricted audience (e.g., management, regulators, or business partners) and provide detailed information about a service organization's controls and the results of testing against the TSC. In contrast, SOC 3 reports are general-use summaries that offer less detail but can be publicly distributed to demonstrate a high-level commitment to trust and transparency.

[13] A 2021 gap assessment identified SOC engagements, digital acumen, cybersecurity, IT governance, and IT risk and controls as areas of growing importance for accountants that were not covered by a majority of United States accounting undergraduate and graduate programs (AICPA/National Association of State Boards of Accountancy (NASBA) 2021).

regulation (AICPA 2024). A similar focus on key technology topics has been applied by the global Institute of Management Accountants, which describes information systems and data governance as key competencies for accountants in its Competency Framework released in 2023 (Institute of Management Accountants (IMA) 2023).

V. IMPLICATIONS FOR ACCOUNTING RESEARCHERS

Prior Accounting Literature on Data Privacy/Protection Regulation

Accounting researchers first became interested in privacy/data protection regulations in the early 2000s as a way to explore the comparative value of enforced regulation versus naturally emerging conventions engendering commentary on the financial reporting regulations being debated in the United States post-Enron.[14] Jamal, Maier, and Sunder (2003, 2005) leveraged the differing regulatory environments of the European Union and the United States to examine whether codified data protection regimes under the EU Data Protection Directive yielded better privacy practices than the self-regulatory norms prevailing in U.S. e-commerce. These early investigations provided accounting scholars a novel domain to interrogate broader questions about the role of government intervention and the limits of market discipline–insights with direct implications for financial reporting policy.

Beyond this foundational work, the topic of privacy and data protection remained largely untouched in accounting research until recently. However, over the last five years, a stream of research has begun to examine both state-level breach disclosure laws in the United States and global data protection regulations (e.g., the GDPR).

Starting in the United States, Ashraf and Sunder (2023) exploit the staggered adoption of state-level breach disclosure laws from 2002 to 2014 to show that these regulations—although framed as consumer protection measures—reduce firms' cost of equity capital, particularly among those without prior cybersecurity investments, signaling diminished perceived shareholder risk. They also document that firms respond to these laws by hiring cybersecurity officers and boosting IT investment. However, other studies argue that strategic and opportunistic firm behavior can surface in response to these regulatory pressures. Chen, Hilary, and Tian (2024) find that insider selling profits increase following breach disclosure mandates, especially among firms with weak governance or high cyber risk. These behaviors are dampened in environments with stronger enforcement, implying that disclosure laws alone may not prevent managerial rent extraction. Lin and She (2025) further reveal that firms may misreport the discovery date of cyber incidents to delay disclosure, particularly when facing internal control weaknesses or looming regulatory deadlines. Although such delays may allow time for remediation and public reassurance, they raise concerns about transparency, investor fairness, and selective information release. Along the same lines, Ashraf, Jiang, and Wang (2022) examine the timing trade-offs imposed by mandatory disclosure deadlines. Using U.S. state-level variation, they show that deadlines do accelerate breach disclosure (by 90 percent) but also lead to less informative disclosures, suggesting that deadline rigidity may sometimes undermine information quality. Investors react negatively to unjustified delays but are tolerant of delays when they are accompanied by fuller disclosure. Their findings emphasize the policy challenge of balancing speed and substance in cyber incident reporting.

Extending beyond the United States, other recent work has focused on the GDPR as the foundational example of a modernized data protection law. Klein, Manini, and Shi (2022) study the effects of the GDPR and find that firms reorient their board governance to place greater emphasis on cybersecurity. These board-level adjustments lead to fewer subsequent cyberattacks. Maex (2022) extends this work beyond board-level implications, showing that the GDPR also prompts firms to strengthen their broader information systems in ways that enhance internal information quality and, in turn, improve operational efficiency. Nonetheless, the GDPR also imposes substantial costs on firms that, at least in the short run, outweigh the above operational benefits (Maex 2022; Motoki and Pinto 2025).

Collectively, these findings highlight that the costs and benefits of modernized data protection regulations can extend well beyond their primary objective of safeguarding personal data. The breadth of these effects, along with the expansion of these regulations globally, opens up a range of promising avenues for future accounting research.

Areas for Future Research

Implications for Firms' Governance and Operations

Much of the above work has focused on the implications of data protection regulations for firm governance, operations, and financial performance. These studies generally focus on the short-term costs and benefits resulting from the

[14] Literature on the concept of information/data privacy and its implications for enterprises and society is vast. See Pavlou (2011); Boritz and No (2011); Bandara, Fernando, and Akter (2020). Also, see Johnson (2022) for broader discussion of the literature on the economic implications of the GDPR.

adoption and enforcement of the GDPR. However, there are potential avenues for future research that would add context to these initial insights. A few questions that offer fruitful avenues for future accounting research include:

1. Do the long-term benefits (operational or otherwise) of global data protection regulations outweigh the initial compliance costs once firms have adjusted their systems and processes?
2. How do country-specific institutional factors (e.g., digital infrastructure, regulatory environment intensity, legal infrastructure, cultural attitudes toward privacy) moderate the costs and benefits of such regulations?
3. What are the financial, operational, or reputational consequences for firms that fail to comply with data protection requirements?
4. How do firms respond following compliance failures, and what remediation strategies are employed?

The global proliferation of data protection laws—each with different scopes, enforcement regimes, and jurisdictional nuances—offers a unique opportunity for researchers to explore these questions, by exploiting the staggered rollout of regulations for cross-country analyses. This variation allows for identification strategies similar to those used in prior international work on other global regulatory changes (e.g., IFRS adoption, executive compensation disclosure mandates, environmental, social, and governance (ESG) reporting).[15] This consideration is particularly relevant since recent privacy regulations outside of GDPR have received little attention in accounting research. Notably these questions can now be addressed through longitudinal analyses that extend beyond the years confounded by the COVID-19 pandemic.

Importantly, many of the operational and governance changes triggered by data privacy laws that would be of interest to accountants may not be observable through traditional public disclosures. As such, qualitative research could play a critical role in uncovering the internal processes, adaptations, and strategic considerations that shape how firms manage information in response to privacy regulation.

Implications for Firm Disclosures and Information Sharing

Privacy regulations may lead firms to adopt a "culture of privacy" (IAPP 2020). To the extent that there is a tightening of control over sensitive information held by the firm, it is not farfetched to consider that there might be a chilling of overall disclosure due to increased legal scrutiny over what is shared publicly. It would be interesting to understand how changes in privacy policies publicized by firms correlate with changes in disclosure transparency, around the adoption of modern privacy regulations that lead firms to adopt such a culture of privacy.[16] Or, more broadly stated:

5. Do data protection regulations lead to changes in firm disclosure transparency as reflected in financial reporting?

Additionally, because requirements for more timely public disclosure of cyber breaches have been shown to reduce the level of detail provided in those disclosures, there is growing concern that such mandates may create unintended consequences. Particularly concerning is the potential dampening effect these regulations may have on cybersecurity information sharing among firms, industry groups, and public-private partnerships, a risk that has been specifically raised in connection with the SEC's 2023 cybersecurity disclosure requirements (Gerding 2024). Firms may worry that sharing threat intelligence or breach details behind the scenes, even in good faith, could later be used as evidence that they withheld material information from investors.[17] To the extent that information sharing is suppressed, it could hinder cybersecurity risk management efforts by organizations and individuals who rely on timely and complete information about active threats. Hence, the following question is a worthy avenue for future research:

6. Do mandatory cybersecurity breach disclosure requirements discourage information sharing among firms and other stakeholders, thereby undermining collective cybersecurity risk management efforts?

Implications for Assurance in Response to Regulatory Requirements

Previous studies have documented the development of standards around data privacy and related mechanisms for assurance. Toy and Hay (2015) provide an overview of the early stages of the privacy assurance ecosystem, describing assurance, attestation, and agreed-upon procedures engagements that used a diverse set of evaluation criteria, including

[15] See, for example, Cascino et al. (2023); He, Shi, Zhou, and Zhu (2025); and Jona and Srivastava (2025) for discussions of some of these global regulatory trends.

[16] Although privacy policies have traditionally been a focus of legal and information systems research, Gao and Brink (2019) explore these from a disclosure standpoint providing a framework for integrating these policies into accounting research.

[17] Such a finding would be consistent with studies documenting a chilling effect on private information sharing following Regulation Fair Disclosure (FD). See Koch, Lefanowicz, and Robinson (2013) for a review of the literature on Regulation FD. Nevertheless, examining whether cybersecurity disclosure requirements produce similar effects remains important given key differences between the two contexts. In particular, the materiality of cybersecurity information is often more difficult to assess, and the operational benefits of sharing threat intelligence (such as improved collective defense) are not present for the financial disclosures governed under Regulation FD.

specific privacy regulations. At the time, they noted that the "inconsistency of standards reduces international comparability of privacy audits, thereby lowering their potential value to the entities subject to audit, and to users of the reports" (Toy and Hay 2015, 181). However, as data protection regulations have become more omnipresent, exploring the development of assurance offerings in the space of personal data protection would be an interesting research avenue. It would also extend recent survey work on the marketplace for emerging assurance services (Bauer et al. 2024). Such offerings may include both standalone privacy assessments by firms under any of a variety of privacy frameworks (e.g., the NIST Privacy Framework, ISO/IEC 27701) and/or the inclusion of the Trust Services Criteria of privacy in reporting under the AICPA's SOC 2/3 framework. Potential research questions include:

7. What is the market structure for firms delivering these assurance services?
8. What factors are associated with the receipt and disclosure of privacy-related assurance services?
9. Which stakeholders, if any, value the receipt and disclosure of privacy-related assurance services by firms?

Studies addressing these research questions could build upon recent work by Schoenfeld (2024) and Qian (2024) that have begun to explore the implications of receiving and disclosing SOC reports.[18] One notable challenge in studying the development of privacy assessments *en masse* is that many of these assessments are not publicized outside of the firm (or are shared only with customers). However, SOC 3 reports, which are intended to be public-facing summaries of SOC 2 reports, may provide an avenue for researchers to explore the evolution of assurance in this space.

VI. CONCLUSION

The evolving landscape of data protection and related regulations presents both challenges and opportunities for management, the accounting profession, and regulators, especially in the realms of information integrity, disclosure practices, and assurance mechanisms. As firms grapple with the demands of compliance and the necessity of safeguarding sensitive personal information, they are compelled to invest in robust governance frameworks, enhance their information management systems, and foster a culture of privacy throughout their organizations. Further, the patchwork of regulations that continue to emerge across global jurisdictions, as well as their interfaces with technologies such as AI and social media, amplify the importance of this area.

As a field focused on understanding how information is managed and communicated by firms, accountants have a sizeable role to play in understanding and responding to this shifting regulatory terrain. This commentary is intended to provide accountants with an overview of the landscape and stimulate discussion on the ways in which the field might play a role in the realms of both practice and research.

DECLARATION OF GENERATIVE AI AND AI-ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this work, the authors used ChatGPT and Microsoft Copilot to refine the writing of the manuscript. After using these tools/services, the authors reviewed and edited the content as needed and take full responsibility for the content of the manuscript.

REFERENCES

AICPA. 2023. *SOC Survey Results Point to the Value of SOC 1 and 2 Engagements*. Durham, NC: AICPA. https://www.aicpa-cima.com/resources/download/soc-survey-results-point-to-the-value-of-soc-1-and-2-engagements

AICPA. 2024. *Uniform CPA Examination Blueprints*. Durham, NC: AICPA. https://www.aicpa-cima.com/resources/download/learn-what-is-tested-on-the-cpa-exam

AICPA. 2025. *CPA Evolution*. Durham, NC: AICPA. https://evolutionofcpa.org/

AICPA/National Association of State Boards of Accountancy (NASBA). 2021. Accounting Program Curriculum Gap Analysis Report. Durham, NC: AICPA. https://www.evolutionofcpa.org/Documents/Accounting%20Program%20Curriculum%20Gap%20Analysis%20Report%203.15.2021.pdf

Ashraf, M., and J. Sunder. 2023. Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review* 98 (4): 1–32. https://doi.org/10.2308/TAR-2020-0787

Ashraf, M., J. Jiang, and I. Y. Wang. 2022. Are there trade-offs with mandating timely disclosure of cybersecurity incidents? Evidence from state-level data breach disclosure laws. *The Journal of Finance and Data Science* 8: 202–213. https://doi.org/10.1016/j.jfds.2022.08.001

[18] Schoenfeld (2024) surveys the receipt of SOC audits by firms but does not differentiate between those focused on internal controls over financial reporting—SOC1 audits—and those focused on security and privacy—SOC 2/3 audits. Qian (2024) explores the value of SOC 2 audits to the liquidity of cryptocurrency exchanges.

Bandara, R., M. Fernando, and S. Akter. 2020. Privacy concerns in e-commerce: A taxonomy and a future research agenda. *Electronic Markets* 30 (3): 629–647. https://doi.org/10.1007/s12525-019-00375-6

Bauer, T. D., J. E. Boritz, K. Fiolleau, B. Pomeroy, A. Vitalis, and P. Wang. 2024. Cataloging the marketplace of assurance services. *Auditing: A Journal of Practice & Theory* 43 (3): 49–75. https://doi.org/10.2308/AJPT-2022-196

Boritz, J. E., and W. G. No. 2011. E-Commerce and privacy: Exploring what we know and opportunities for future discovery. *Journal of Information Systems* 25 (2): 11–45. https://doi.org/10.2308/isys-10090

Cascino, S., H. Daske, M. DeFond, A. Florou, J. Gassen, and M. Hung. 2023. Reflections on the 20-year anniversary of worldwide IFRS adoption. *Journal of International Accounting Research* 22 (3): 85–96. https://doi.org/10.2308/JIAR-2023-037

Chander, A., M. E. Kaminski, and W. McGeveran. 2021. Catalyzing privacy law. *Minnesota Law Review* 105 (4): 1733–1802. https://minnesotalawreview.org/article/catalyzing-privacy-law/

Chen, J., E. Henry, and X. Jiang. 2023. Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics* 187 (1): 199–224. https://doi.org/10.1007/s10551-022-05107-z

Chen, X., G. Hilary, and X. Tian. 2024. Mandatory data breach disclosure and insider trading. *Journal of Business Finance & Accounting*. https://doi.org/10.1111/jbfa.12842

Cheong, A., K. Yoon, S. Cho, and W. G. No. 2021. Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems* 35 (2): 179–194. https://doi.org/10.2308/ISYS-2020-031

Chin-Rothmann, C. 2019. Highlights: The GDPR and CCPA as benchmarks for federal privacy legislation. https://www.brookings.edu/articles/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/

Department for Science, Innovation, and Technology (DSIT). 2025. Research into the prevalence and quality of cyber disclosures. https://www.gov.uk/government/publications/research-on-the-prevalence-and-quality-of-cyber-disclosures

DLA Piper. 2025. Data protection laws of the world. https://www.dlapiperdataprotection.com/

EU AI Act. 2025. Up-to-date developments and analyses of the EU AI Act. https://artificialintelligenceact.eu/

European Commission. 2025. NIS2 directive: New rules on cybersecurity of network and information systems. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Financial Reporting Council (FRC). 2024. Corporate governance code guidance. https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/corporate-governance-code-guidance/

Flexera. 2019. 2019 RightScale State of the Cloud Report. Itasca, IL: Flexera. https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf

Florackis, C., C. Louca, R. Michaely, and M. Weber. 2023. Cybersecurity risk. *The Review of Financial Studies* 36 (1): 351–407. https://doi.org/10.1093/rfs/hhac024

Freese, J. 1977. The Swedish Data Act. *Current Sweden* 178: 1–8.

Gao, L., and A. G. Brink. 2019. A content analysis of the privacy policies of cloud computing services. *Journal of Information Systems* 33 (3): 93–115. https://doi.org/10.2308/isys-52188

GDPR Enforcement Tracker. 2025. Fines statistics. https://www.enforcementtracker.com/?insights

Gerding, E. 2024. Selective disclosure of information regarding cybersecurity incidents. https://www.sec.gov/newsroom/whats-new/gerding-cybersecurity-incidents-06202024

Gilchrist, K. 2018. Apple's Tim Cook: 'Don't believe' tech companies that say they need your data. *CNBC* (October 3). https://www.cnbc.com/2018/10/03/apple-ceo-tim-cook-dont-believe-tech-claims-about-personal-data.html

Greenleaf, G. 2013. Global tables of data privacy laws and bills (3rd ed, June 2013). (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875

Greenleaf, G. 2023. Global tables of data privacy laws and bills (8th ed.) 2023. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4405514

Greenleaf, G. 2025. Global data privacy laws 2025: 172 countries, twelve new in 2023/24. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5275559

Hartzog, W., and N. Richards. 2020. Privacy's constitutional moment and the limits of data protection. *Boston College Law Review* 61 (5): 1687–1761. https://bclawreview.bc.edu/articles/205

He, C., H. Shi, G. Zhou, and X. Zhu. 2025. Say-on-pay laws and financial reporting quality around the world: Evidence from a natural experiment. *Journal of International Accounting Research* 24 (1): 47–70. https://doi.org/10.2308/JIAR-2022-050

IAPP. 2020. Building a culture of privacy: Legal compliance as a result, not a goal. https://iapp.org/news/a/building-a-culture-of-privacy-legal-compliance-as-a-result-not-a-goal

IAPP. 2025. About the IAPP. https://iapp.org/about/what-is-privacy/

IBM. 2025. What is data protection? https://www.ibm.com/think/topics/data-protection

Institute of Management Accountants (IMA). 2023. IMA management accounting competency framework. https://mc-69e30ef4-758e-4371-ac6f-2657-cdn-endpoint.azureedge.net/-/media/IMA/Files/Home/Career-Resources/Management-Accounting-Competencies/IMA-Framework-11-28-23.ashx?rev=7eebd63ad50e47bc8d6d9c0d7b9185f1

Jamal, K., M. Maier, and S. Sunder. 2003. Privacy in e-commerce: Development of reporting standards, disclosure, and assurance services in an unregulated market. *Journal of Accounting Research* 41 (2): 285–309. https://doi.org/10.1111/1475-679X.00104

Jamal, K., M. Maier, and S. Sunder. 2005. Enforced standards versus evolution by general acceptance: A comparative study of e-commerce privacy disclosure and practice in the United States and the United Kingdom. *Journal of Accounting Research* 43 (1): 73–96. https://doi.org/10.1111/j.1475-679x.2004.00163.x

Johnson, G. 2022. Economic research on privacy regulation: Lessons from the GDPR and beyond. (Working paper). https://www.nber.org/papers/w30705

Jona, J., and A. Srivastava. 2025. A discussion on the global trend of climate-risk disclosures. *Journal of International Accounting Research* (forthcoming). https://doi.org/10.2308/JIAR-2025-002

Klein, A., R. Manini, and Y. Shi. 2022. Across the pond: How US firms' boards of directors adapted to the passage of the general data protection regulation. *Contemporary Accounting Research* 39 (1): 199–233. https://doi.org/10.1111/1911-3846.12735

Knechel, W. R. 2021. The future of assurance in capital markets: Reclaiming the economic imperative of the auditing profession. *Accounting Horizons* 35 (1): 133–151. https://doi.org/10.2308/HORIZONS-19-182

Koch, A. S., C. E. Lefanowicz, and J. R. Robinson. 2013. Regulation FD: A review and synthesis of the academic literature. *Accounting Horizons* 27 (3): 619–646. https://doi.org/10.2308/acch-50500

KPMG UK. 2024. KPMG Controls Assurance Benchmarking Report 2024. London, U.K.: KPMG UK. https://assets.kpmg.com/content/dam/kpmgsites/uk/pdf/2024/10/soc-reporting-benchmarking.pdf

Li, H., W. G. No, and T. Wang. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems* 30: 40–55. https://doi.org/10.1016/j.accinf.2018.06.003

Lin, X., and G. She. 2025. Timely cybersecurity disclosure and information manipulation. *Management Science* 71 (11): 9308–9327. https://doi.org/10.1287/mnsc.2023.01058

Locke, J. 1988. *Two Treatises on Government*, edited by P. Laslett. Cambridge, U.K.: Cambridge University Press.

Maex, S. 2022. Modern privacy regulation, internal information quality, and operating efficiency: Evidence from the general data protection regulation. https://doi.org/10.34944/dspace/8025

McClain, C., M. Faverio, M. Anderson, and E. Park. 2023. How Americans view data privacy. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

Milmo, D. 2022. France fines Google and Facebook €210m over user tracking. *The Guardian* (January 6). https://www.theguardian.com/technology/2022/jan/06/france-fines-google-and-facebook-210m-over-user-tracking-cookies

Motoki, F., and J. Pinto. 2025. Regulating data: Evidence from corporate America. *Journal of Business Finance & Accounting* 52 (1): 541–568. https://doi.org/10.1111/jbfa.12820

OECD. 2002. OECD guidelines on the protection of privacy and transborder flows of personal data. Originally adopted September 23, 1980. https://www.oecd.org/en/publications/2002/02/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_g1gh255f.html

OECD. 2025. OECD AI principles overview. https://oecd.ai/en/ai-principles

Page, C. 2020. Marriott hit with £18.4 million GDPR fine over massive 2018 data breach. *Forbes* (October 30). https://www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/

Pavlou, P. 2011. State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly* 35 (4): 977–988. https://doi.org/10.2307/41409969

Qian, J. 2024. The value of auditor assurance in cryptocurrency trading. (Working paper). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4536274

Schoenfeld, J. 2024. Cyber risk and voluntary service organization control (SOC) audits. *Review of Accounting Studies* 29 (1): 580–620. https://doi.org/10.1007/s11142-022-09713-0

SEC. 2011. CF Disclosure Guidance: Topic No. 2—Cybersecurity. Washington, DC: SEC. https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

SEC. 2023. Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Washington, DC: SEC. https://www.sec.gov/rules-regulations/2023/07/s7-09-22

Toy, A., and D. C. Hay. 2015. Privacy auditing standards. *Auditing: A Journal of Practice & Theory* 34 (3): 181–199. https://doi.org/10.2308/ajpt-50932

United Nations. 1948. *Universal Declaration of Human Rights*. Paris, France: United Nations.

United Nations. 1966. *International Covenant on Civil and Political Rights*. New York, NY: United Nations.

United States Department of Health, Education, and Welfare (US DHEW). 1973. Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Washington, DC: DHEW. https://www.justice.gov/opcl/docs/rec-com-rights.pdf

United States Office of Privacy and Civil Liberties (US OPCL). 2022. *Overview of The Privacy Act of 1974 (2020 Edition)*. Washington, DC: DOJ. https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

Warren, S. D., and L. D. Brandeis. 1890. The right to privacy. *Harvard Law Review* 4 (5): 193–220. https://doi.org/10.2307/1321160

APPENDIX A

Examples of Cybersecurity Risk Factor Disclosures Referencing Privacy Regulations (in United States 10-K Filings)

FY 2017 10-K for Eastman Kodak Company

(https://www.sec.gov/Archives/edgar/data/31235/000156459018005857/kodk-10k_20171231.htm)

Improper disclosure of personal data could result in liability and harm Kodak's reputation. (emphasis added)

Kodak receives, processes, transmits and stores information relating to identifiable individuals (personal information), both in its role as a technology provider and as an employer. *As a result, Kodak is subject to numerous U.S. federal and state and foreign laws and regulations relating to personal information. These laws have been subject to frequent changes, and new legislation in this area may be enacted at any time.* ***In Europe, the General Data Protection Regulation (GDPR) will become effective on May 25, 2018 for all European Union (EU) member states. The GDPR will include operational requirements for companies receiving or processing personal data of EU residents that are partially different from those currently in place, and will include significant penalties for noncompliance. This change, as well as any other change to existing laws, the introduction of new laws in this area, or the failure to comply with existing laws that are applicable, may subject Kodak to, among other things, additional costs or changes to its business practices, liability for monetary damages, fines andlor criminal prosecution, unfavorable publicity, restrictions on its ability to obtain and process information and allegations by its customers and clients that it has not performed its contractual obligations.*** At the same time, the risk of cyber-attacks is relevant to the requirements regarding storage, transfer, sharing and handling of personal information. This environment demands Kodak continuously improve its design and coordination of security controls and contractual arrangements across its businesses and geographies. Despite these efforts, it is possible its security controls over personal data, its training of employees and vendors on data privacy and data security, and other practices it follows may not prevent the improper disclosure of personal information. Improper disclosure of this information could harm its reputation or subject it to liability under laws which protect personal data, resulting in increased costs or loss of revenue. (emphasis added)

FY 2017 10-K for Levi Strauss & Co.

(https://www.sec.gov/Archives/edgar/data/94845/000009484518000013/a2017yeform10-k.htm)

We face cybersecurity risks and may incur increasing costs in an effort to minimize those risks. (emphasis added)

We utilize systems and websites that allow for the secure storage and transmission of proprietary or confidential information regarding our consumers, employees, and others, including credit card information and personal information. As evidenced by the numerous companies who have suffered serious data security breaches, we may be vulnerable to, and unable to anticipate or detect data security breaches and data loss, including rapidly evolving and increasingly sophisticated cybersecurity attacks. In addition, data security breaches can also occur as a result of a breach by us or our employees or by persons with whom we have commercial relationships that result in the unauthorized release of personal or confidential information. In addition to our own databases, we use third-party service providers to store, process and transmit confidential or sensitive information on our behalf. Although we contractually require these service providers to implement and use reasonable security measures, we cannot control third parties and cannot guarantee that a data security breach will not occur in the future either at their location or within their systems.

A data security breach may expose us to a risk of loss or misuse of this information, and could result in significant costs to us, which may include, among others, potential liabilities to payment card networks for reimbursement of credit card fraud and card reissuance costs, including fines and penalties, potential liabilities from governmental or third-party investigations, proceedings or litigation and diversion of management attention. We could also experience delays or interruptions in our ability to function in the normal course of business, including delays in the fulfillment or cancelation of customer orders or disruptions in the manufacture and shipment of products. In addition, actual or anticipated attacks may cause us to incur costs, including costs to deploy additional personnel and protection technologies, train employees, and engage third-party experts and consultants. Any compromise or breach of our security could result in a violation of applicable privacy and other laws, significant legal and financial exposure, and a loss of confidence in our security measures, which could have an adverse effect on our results of operations and our reputation.

In addition, the regulatory environment surrounding information security and privacy is increasingly demanding, with frequent imposition of new and changing requirements. For example, the European Union's General Data Protection Regulation ("GDPR"), which will become effective in May 2018, imposes significant new requirements on how we collect, process and transfer personal data, as well as significant fines for noncompliance. Compliance with changes in privacy and information security laws and standards may result in significant expense due to increased investment in technology and the development of new operational processes. (emphasis added)

FY 2019 10-K La-Z-Boy Incorporated

(https://www.sec.gov/Archives/edgar/data/57131/000104746919003700/a2239055z10-k.htm)

Our business and our reputation could be adversely affected by cybersecurity incidents and the failure to protect sensitive employee, customer, consumer, vendor or Company data, or to comply with evolving regulations relating to our obligation to protect such data. (emphasis added)

(continued on next page)

APPENDIX A (continued)

Cyber-attacks designed to gain access to sensitive information by breaching security systems of large organizations leading to unauthorized release of confidential information have occurred over the last several years at a number of major U.S. companies. Despite widespread recognition of the cyber-attack threat and improved data protection methods, cyber-attacks on organizations continue to be persistent and ever-changing, making it difficult to prevent and detect these attacks. Similar to many other retailers, we receive and store certain personal information about our employees, customers, consumers, and vendors. Additionally, we rely on third-party service providers to execute certain business processes and maintain certain information technology systems and infrastructure, and we supply such third-party providers with the personal information required for those services.

States and the federal government are increasingly enacting laws and regulations to protect consumers against identity theft, and in the future we may be subject to state or federal data privacy laws, such as the California Consumer Privacy Act of 2018 (the "CCPA"). We are also subject to data privacy and other similar laws and regulations in various foreign jurisdictions, such as the European Union. These laws and regulations are emerging and evolving in various countries and the interpretation and application of these laws and regulations in the United States, Europe and elsewhere often are uncertain, contradictory and changing. For example, the European General Data Protection Regulation (GDPR) applies to us, creating a range of new compliance obligations regarding the treatment of personal data. In addition, the GDPR contains significant penalties for noncompliance. It is possible that these laws may be interpreted or applied in a manner that is adverse to us, unforeseen, or otherwise inconsistent with our practices or that we may not adequately adapt our internal policies andlor procedures to evolving regulations, any of which could result in litigation, regulatory investigations and potential legal liability, require us to change our practices in a manner adverse to our business or limit access to our products and services in certain countries. As a result, our reputation and brand, which is critical to our business operations, may be harmed, we could incur substantial costs, and we could lose both consumers and revenue. (emphasis added)

During fiscal 2019, we were subject, and will likely continue to be subject, to attempts to breach the security of our networks and IT infrastructure through cyber-attack, malware, computer viruses, and other means of unauthorized access. To the best of our knowledge, attempts to breach our systems have not been successful to date. A breach of our systems that results in the unauthorized release of sensitive data could adversely affect our reputation resulting in a loss of our existing customers and potential future customers, lead to financial losses due to remedial actions or potential liability, possibly including punitive damages, or we could incur regulatory fines or penalties. An electronic security breach resulting in the unauthorized release of sensitive data from our information systems or those of our third party service providers could also materially increase the costs we already incur to protect against these risks. We continue to balance the additional risk with the cost to protect us against a breach, and have taken steps to ensure that losses arising from a breach would be covered in part by insurance that we carry.