MASTER THESIS

„Protecting Consumers from Data Breaches: Regulatory Approaches in the European Union, United States, and India“

verfasst von / submitted by

Emily Pehrsson

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2019 / Vienna 2019

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	A 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor:	Siegfried Fina

Table of Contents

List of Abbreviations

CCPA	California Consumer Privacy Act, 2018
CIDR	Central Identities Data Repository
DDoS	Distributed-Denial-of-Service
ENISA	European Union Agency for Network and Information Security
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulation
GLBR	Gramm-Leach-Bliley Act
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
IoT	Internet of Things
IT Act	Information Technology Act
NIS	Network and Information Systems
PDPB	Personal Data Protection Bill
UIDAI	Unique Identification Authority of India
WP29	Article 29 Working Party

1. Introduction

As economies around the world increasingly rely on the Internet of Things (IoT), monetized consumer data, and the internet more generally, the risks posed by a cybersecurity incident have intensified. In the last decade, a seemingly unending stream of large-scale corporate data breaches impacting millions of consumers has prompted a consumer protection movement around cybersecurity issues. Regulators worldwide have responded to public outrage by promulgating new regulations governing corporations' cybersecurity standards. These regulations are primarily intended to reduce the number and severity of data breaches and improve protections for consumer data stored and processed by private-sector organizations. Approaches, however, have varied substantially, creating a complex patchwork of regulation for companies operating globally.

Given the relatively new nature of this threat and its rapid evolution, regulators have not reached a consensus on the most effective methods of ensuring cybersecurity in the private sector. While this wide range of cybersecurity approaches offers an opportunity to critically assess the effectiveness of each, it poses a major obstacle for multinational corporations. Inconsistent regulations increase the complexity, and thus the cost, of compliance. The purpose of this paper is to survey recently implemented cybersecurity regulations in three major markets: the European Union, the United States, and India. It will highlight different approaches to promoting companies' security standards with regard to their data processing activities.

Following the introduction, this paper will consist of five parts. Part 2 will examine the changing threat landscape in the cyber domain, highlighting major trends in the method and frequency of cyber incidents. Part 3 will examine the EU's regulatory approach, focusing on the General Data Protection Regulation (GDPR), which entered into force in 2018. Part 4 will analyze the United States' piecemeal approach to regulation, based in its federalist system. This section will focus on the California Consumer Privacy Act (CCPA), signed into law in 2018. Part 5 will assess India's proposed Personal Data Protection Bill, initially proposed in 2018, but expected to be re-introduced in an altered form following India's 2019 elections. Part 6 will compare key provisions from these three markets, discussing their relative strengths and weaknesses. It will also recommend amendments to the existing laws and strategies that should be incorporated into future legislation.

2. Proliferating Threats

The severity and frequency of corporate cyber incidents has persisted, even as the public and private sectors alike pour millions of dollars into cybersecurity and data protection initiatives. Innovative cyber criminals continually develop new and more sophisticated ways of penetrating networks and compromising data, contributing to this problem.[1] Interestingly, however, evolving techniques alone are not to blame. According to a recent cybersecurity study, traditional, years-old cyber-attack strategies were still successful against a small, but substantial portion of employees. In 2018, approximately 4% of employee targets fell for phishing campaigns by clicking on an infected link.[2] Consequently, cybersecurity strategies require a combination of innovation and repetitive employee training to minimize threats to consumers' data.

A key challenge in the cybersecurity field is the broad range of possible threats, making definition, let alone prevention, difficult. An estimated 73% of cyber incidents were perpetrated by external actors, about half of whom were affiliated with organized criminal groups.[3] The remaining 28% of incidents, however, are considered "internal"—meaning that they were caused by an organization's employees, whether intentionally or unintentionally.[4] Typically, such "insider threats" are much more difficult to prevent and detect, because they require cybersecurity personnel or systems to distinguish between an employee accessing data to perform her job on the one hand, and to compromise the company's data on the other.[5]

Furthermore, cyber incidents can take a myriad of forms, from malware to distributed-denial-of-service (DDoS) attacks to Advanced Persistent Threats, or a combination thereof. Ransomware attacks were a major cybersecurity threat for companies in 2018.[6] For this type of attack, the perpetrator will typically send an employee an email with an attachment containing

---

[1] *See, e.g.,* Ciara Byrne, 'The new ways we could get hacked (and defended) in 2019' *Fast Company* (7 Jan. 2019) <https://www.fastcompany.com/90287253/cybersecurity-cybercrime-threats-defenses-2019> accessed 24 Apr. 2019; Lily Hay Newman, 'The Year Cryptojacking Ate the Web' *Wired* (24 Dec. 2018) <https://www.wired.com/story/cryptojacking-took-over-internet/> accessed 24 Apr. 2019.

[2] 2018 Data Breach Investigations Report: Executive Summary (Verizon 2018) <https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report_execsummary.pdf> accessed 24 Apr. 2019, 3.

[3] Ibid 2.

[4] Ibid.

[5] *See* Tripwire Guest Authors, 'Insider Threats as the Main Security Threat in 2017' *Tripwire* (11 Apr. 2017) <https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/> accessed 24 Apr. 2019.

[6] *See* Kate O'Flaherty, 'How to Survive a Ransomware Attack—And Not Get Hit Again' *Forbes* (17 August 2018) <https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#fa945c26cd36> accessed 23 May 2019.

malware. When the employee downloads the malicious content, the perpetrator can gain access to segments of the company's data and take control. She can lock legitimate employees out of the network, threatening to delete or continue denying access to the data unless the company pays a "ransom" in cryptocurrency.[7] Some estimates place the aggregate cost of ransomware as high as USD $11.9 billion in 2019.[8] By contrast, a DDoS attack starts when a malicious actor uses malware to gain control of multiple computers, creating what is called a botnet. The perpetrator can then direct the botnet to overwhelm a target computer or network with requests. The overloaded target is unable to process any legitimate requests, because it is flooded with illegitimate ones.[9] DDoS attacks paralyze the target company for the duration of the "assault"—while the DDoS attack continues, an online retailer might be prevented from selling its goods, for example.[10] The cost of a DDoS attack is estimated to range between USD $50,000 and $2.5 million.[11]

Regulating cybersecurity uniformly across the private sector can also pose a major challenge because the nature and target of threats vary by industry. For example, in the accommodations industry, the vast majority of cyber incidents are the result of an external actor—an estimated 99%.[12] 93% of cyber incidents were targeting customers' payment systems.[13] The healthcare industry, however, faces a completely different spectrum of threats to consumers' data. 56% of cyber incidents in healthcare are the result of an internal actor—a combination of employees' mistakes and willful misuse of data.[14] Rather than payment data, medical data tends to be at risk.[15] From these two examples, the difficulty of regulating this field becomes much clearer: the risks are varied; the actors are a combination of unknown external actors and a company's own

[7] Comodo, 'Ransomware Threats and Endpoint Security – An Overview' *Comodo Security Solutions* (12 Apr. 2018), <https://enterprise.comodo.com/blog/ransomware-threats-and-endpoint-security-overview/> accessed 24 Apr. 2019.
[8] Steve Morgan, 'Ransomware damage costs predicted to hit $11.5B by 2019' *CSO* (20 Nov. 2017) <https://www.csoonline.com/article/3237674/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html> accessed 24 Apr. 2019.
[9] CISA, 'Security Tip (ST04-015) Understanding Denial-of-Service Attacks' (*Cybersecurity and Infrastructure Security Agency (CISA)* 28 June 2018) <https://www.us-cert.gov/ncas/tips/ST04-015> accessed 24 Apr. 2019.
[10] *See* Steve Patton, 'What is the Real Cost of a DDoS Attack?' *IoT Tech Expo* (16 Oct. 2018) <https://www.iottechexpo.com/2018/10/iot/what-is-the-real-cost-of-a-ddos-attack/> accessed 24 Apr. 2019.
[11] Ibid.
[12] 2018 Data Breach Investigations Report: Executive Summary, 4.
[13] Ibid.
[14] Ibid 5.
[15] Ibid.

employees; the methods are evolving and diverse; and multiple pools of data can be at risk at different times.

The public sector has a vested interest in the cyber resilience of the private sector, beyond its obligation to safeguard the interests of its constituency. Public sector programs often must rely on private sector partners to implement state-sponsored programs or partner on government initiatives. India's nationwide identification program, Aadhaar, is one example. Aadhaar is a program administered by the Unique Identification Authority of India (UIDAI).[16] Indian residents offer a combination of demographic and biometric data, which is stored in a government database. They are then issued an identification number and card, which can be used to authenticate their identity for various purposes.[17] Aadhaar relies heavily on private sector contractors, reducing costs by encouraging corporations to compete for the work.[18] While this model has benefits, it also increases risks for Aadhaar users' data. Insider threats pose a risk to the data, in part because several key contractors have current or past ties to foreign intelligence agencies.[19] Additionally, India currently lacks a comprehensive data protection or cybersecurity regulation; while the Aadhaar Act of 2016 established some standards for the handling of data, sharing users' data with more partners can increase the risk of a data breach.[20]

India is certainly not the only government relying heavily on contractors to perform government functions. In the fiscal year 2017, the U.S. government spent approximately USD $500.9 billion on contracts, including with companies such as Northrop Grumman, Lockheed Martin, The Mitre Corporation, and McKesson Corporation.[21] Responding to cybersecurity concerns relating to its federal contractors, the federal government in 2018 ramped up

[16] UIDAI, 'What Is Aadhaar?' <https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html> accessed 24 Apr. 2019.
[17] Ibid.
[18] *See* Alan Gelb & Julia Clark, 'Performance Lessons from India's Universal Identification Program' *Center for Global Development* (May 2013) < https://www.cgdev.org/sites/default/files/biometric-performance-lessons-India.pdf> accessed 25 Apr. 2019, 9.
[19] Govind Krishnan, 'Foreign agencies can access Aadhaar data' *Sunday Guardian* (Bangalore, 25 Dec. 2011) <http://www.sunday-guardian.com/investigation/foreign-agencies-can-access-aadhar-data> accessed 25 Apr. 2019.
[20] *See* 'Learning with the Times: What is Aadhaar?' *The Times of India* (3 Oct. 2010) <https://timesofindia.indiatimes.com/india/Learning-with-the-Times-What-is-Aadhaar/articleshow/6680601.cms> accessed 25 Apr. 2019; The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, INDIA CODE (2016), preamble (Aadhaar Act) §§ 28-33.
[21] *See* 'Contract Explorer Sunburst,' *Data Lab* (Dec. 2017) < https://datalab.usaspending.gov/contract-explorer.html?search=Contract%20spending%20in%20Fiscal%20Year%202017> accessed 25 Apr. 2019.

cybersecurity requirements for its private sector partners.[22] Measures include implementing cybersecurity audits and using the contractor's cybersecurity capabilities as an evaluation criterion in contract awards.[23] The 2018 breach of 1.5 million patients' healthcare data illustrates the full scope of the risk. The massive breach was the result of a cyberattack on Singapore's healthcare system.[24] Two government-owned corporations, SingHealth and Integrated Health Information Systems (IHiS), were held responsible.[25]

It is not only regulators that are concerned about the cybersecurity threat landscape, however. The Ponemon Institute reported that 66% of high-ranking IT professionals in the private sector predict that their company's shareholder value will decrease as a result of cyber incidents.[26] Recent data substantiates this fear. Companies falling victim to a major cybersecurity breach experienced, on average, a 1.8% permanent drop in their share price.[27] As a result of the increasing risk and consequences of a cybersecurity breach, spending has substantially increased. Worldwide spending on cybersecurity, including private and public entities, increased 12.4% to $114 billion in 2018, and is anticipated to increase again by 8.7% to $124 billion in 2019.[28] Approximately $3.5 billion of this spending will be on data protection in 2019.[29] A loss of consumer trust in a brand can be costly. In a 2017 survey, 62% of consumers indicated that they would blame the company that was breached for the loss of their data more than they would even

[22] Tina Reynolds, 'Government Contracts Insights," *Morrison & Foerster* (25 Jan. 2018) <http://govcon.mofo.com/defense/top-five-government-contractor-cybersecurity-considerations-for-2018/> accessed 25 Apr. 2019.
[23] Ibid.
[24] *See* Irene Tham, 'Singapore's privacy watchdog fines IHiS $750,000 and SingHealth $250,000 for data breach,' *The Straits Times* (15 Jan. 2019) <https://www.straitstimes.com/singapore/singapores-privacy-watchdog-fines-ihis-750000-singhealth-250000-for-data-breach> accessed 25 Apr. 2019.
[25] Ibid.
[26] '2018 Study on Global Megatrends in Cybersecurity' *Ponemon Institute LLC* (Feb. 2018) <https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf> accessed 24 Apr. 2019, 1.
[27] *Reuters*, 'Cyber Breaches Cause Permanent Damage to Share Values' *Fortune* (12 Apr. 2017) <http://fortune.com/2017/04/12/cyber-breaches-shareholder-damage/> accessed 24 Apr. 2019.
[28] Susan Moore & Emma Keen, 'Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019' *Gartner* (Sydney, 15 Aug. 2018) <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019> accessed 24 Apr. 2019.
[29] Ibid.

blame the hacker.[30] 78% of survey respondents in 2018 indicated that they would stop interacting with a company's online platform if it was the subject of a cybersecurity breach.[31]

Consumer sentiment varies between countries, however. Americans are much more willing to share sensitive personal information with corporations than citizens of France, Germany, or the UK. Despite Americans having experienced proportionally more data breaches than their European counterparts,[32] they are about two times as likely as the French, nearly three times as Germans, and four times as British to share their sensitive personal information with corporations.[33] These varied reactions between countries' consumer bases have the potential to impact corporations' and legislators' prioritization of cybersecurity in relation to other pressing issues.

Many of us have had the unwelcome experience of receiving a letter in the mail notifying us that our data was part of a security breach. Often, the response to the compromise of our data—whether our medical records, identification number, communications, credit card information, or anything else—felt utterly inadequate. It is a sign of the times that having your personal data compromised by a corporation is nearly universal in developed economies. Surveying the largest data breaches of 2018 demonstrates why: Indane, a state-owned Indian utility company, lost the personal data of 1.1 billion users; Marriott Hotels, 500 million customers; Exactis, a U.S.-based data broker, 340 million; MyFitnessPal, an American health app, 150 million; and Quora, a California-based knowledge-sharing platform, 100 million.[34] This list is far from exhaustive. The recent wave of legislation pertaining to data protection and cybersecurity standards is, in part, a response to rising public distrust that private sector entities will protect consumers' data.

---

[30] Jennifer King, 'Consumers Don't Want Personalization to Get Too Personal' *eMarketer* (26 Apr. 2018) <https://www.emarketer.com/content/consumers-don-t-want-personalization-to-get-too-personal> accessed 24 Apr. 2019.

[31] 'Survey Shows Consumers are Abandoning Brands after Data Breaches' *Security Magazine* (23 Jan. 2019) <https://www.securitymagazine.com/articles/89777-shows-consumers-are-abandoning-brands-after-data-breaches> accessed 24 Apr. 2019.

[32] 27% of Americans have experienced a data breach, compared to 21% of French, 17% of Germans, and 15% of the British. Ibid.

[33] Ibid.

[34] Paige Leskin, 'The 21 Scariest Data Breaches of 2018' *Business Insider* (30 Dec. 2018) <https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12> accessed 24 Apr. 2019.

3. Europe

3.1 The Regulatory Landscape

The European Union made waves around the world with its adoption of the General Data Protection Regulation (GDPR) in 2016, transforming data protection standards for companies operating in the EU.[35] The GDPR, however, is only one of a series of reforms impacting the digital sector. Europe adopted a bundle of cybersecurity initiatives to support its growing digital economy in 2017.[36] As part of this initiative, it allocated additional responsibilities to the European Union Agency for Network and Information Security (ENISA), an organization intended to coordinate between the public and private sector and across EU Member States.[37] For example. ENISA was charged with assisting the EU in managing cross-border cybersecurity incidents, which are likely to become even greater challenges in the future.[38] Thus far, ENISA has had limited effectiveness, due to political and resource constraints.[39] For example, ENISA has struggled to achieve its mission of enhancing EU-wide cybersecurity owing to varied cyber capabilities in different Member States. While Germany and France possess advanced capabilities, many Member States within Eastern and Southern Europe have much more rudimentary capabilities.[40] Furthermore, ENISA has failed to become a reference point and advisor for the private sector.[41] Precisely defining ENISA's role and giving it the tools necessary to be effective is particularly difficult in light of the EU's character as a supranational organization. The Member States and EU government sometimes develop a contentious relationship in areas of concurrent responsibility, resulting in unclear mandates for EU agencies.

[35] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 ("EU GDPR").
[36] *See* European Commission: Cybersecurity Technology & Capacity Building (Unit H.1), 'Cybersecurity' (16 April 2016) <https://ec.europa.eu/digital-single-market/en/cyber-security> accessed 9 May 2019.
[37] Ibid.
[38] Ibid.
[39] Karin Attström et al., 'Study on the Evaluation of the European Union Agency for Network and Information Security' (*European Commission* 2016) <https://ec.europa.eu/digital-single-market/en/news/final-report-evaluation-european-union-agency-network-and-information-security-enisa> accessed 9 May 2019.
[40] Ibid 5.
[41] Ibid 6.

Passed and implemented in 2016, the NIS Directive required Member States to adopt laws enhancing cybersecurity.[42] It specifically acknowledges, and preserves, sector-specific cybersecurity regulations that impose a standard at least as strict as the NIS Directive.[43] The Directive establishes an "appropriateness" standard of cybersecurity-related conduct for providers of essential services:

> [O]perators of essential services [must] take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.[44]

These operators are explicitly authorized to consider the cost of security measures in light of the risk of a cybersecurity incident. All operators, therefore, are not bound to one designated level of cybersecurity, whether state-of-the-art or a lower standard. Each must rely on its judgment in determining what is appropriate in light of the circumstances—improving flexibility, but decreasing predictability. This standard is duplicated for providers of digital services, but requires the consideration of a variety of other factors, including international security standards.[45]

The NIS Directive also creates a notification scheme at the Member State level. Not all cyber incidents trigger the notification requirement—only those that cause "a significant impact on the continuity of the essential services."[46] This restriction serves a gatekeeping function for the regulator, who can devote fewer resources to sorting the wheat from the chaff, and more to responding to high-risk incidents. The notification must occur "without undue delay," a standard that avoids a rigid timetable, but gives a substantial amount of discretion to the operator to determine what amount of delay may be due.[47] For companies falling into neither the essential nor digital services categories, notification is voluntary.[48]

---

[42] European Commission: Cybersecurity Technology & Capacity Building (Unit H.1), 'The Directive on security of network and information systems (NIS Directive)' (24 August 2018) <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> accessed 9 May 2019.
[43] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [2016] OJ L194/1 ("NIS Directive") rec. 9.
[44] Ibid Art. 14(1).
[45] Ibid Art. 16 (1).
[46] Ibid Art. 14(3).
[47] Ibid.
[48] Ibid Art. 20.

Prior to the 2017 overhaul, the EU passed the eIDAS Regulation in 2014, which created a verification system for online electronic documents across borders.[49] This law was aimed at lowering transaction costs for cross-border enterprises, allowing Europe to compete more effectively with other global powers in the digital marketplace.[50] While all of these components of Europe's cybersecurity plan are interconnected and important in their own right, this paper focuses on the cybersecurity provisions embedded in the GDPR, the most comparable analog to California's new data protection law and India's Personal Data Protection Bill.

Against this backdrop, the GDPR was designed to address concerns about the use and protection of individuals' personal data. The GDPR is deeply controversial around the world due to its stringent penalties, broad extraterritorial application, and complex data processing regulations. Compliance costs for Europe's experiment were astronomical—for example, some reports indicate that over three-quarters of affected companies spent more than USD $1 million on compliance for the GDPR.[51] Such high costs raise the question: were these expenditures worth it? If the GDPR's requirements fail to improve privacy and cybersecurity outcomes, then the opportunity cost of that money was possibly enhanced cybersecurity measures that the companies could have alternatively invested in.

Thus far, however, indications have been positive: "GDPR-ready organizations have also experienced fewer data breaches, and when breaches have occurred, fewer records were impacted, and system downtime was shorter. As a result, the total cost of data breaches was less than what organizations not ready for GDPR experienced."[52] Specifically, Cisco compared the percentage of data breaches experienced by a GDPR-compliant, versus non-compliant, company. 89% of companies that are furthest from GDPR compliance experienced a data breach in the year prior to the study, whereas only 74% of GDPR-compliant companies did.[53] While compliance rates are highest in the EU, approximately 57% of U.S. companies report being

[49] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.
[50] Marina Kirova, 'eIDAS Regulation (Regulation (EU) N°910/2014)' (*European Commission* 2016) <https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014> accessed 9 May 2019.
[51] Josh Fruhlinger, 'Top cybersecurity facts, figures and statistics for 2018' *CSO Online* (10 October 2018) <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html> accessed 9 May 2019.
[52] Cisco, 'Maximizing the value of your data privacy investments Data Privacy Benchmark Study' (January 2019) 2 <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf> accessed 9 May 2019.
[53] Ibid 7.

GDPR-compliant, compared with 60% of Canadian and 65% of Indian companies.[54] Improving data security was one of the top three major challenges companies faced in implementing the GDPR.[55]

The EU itself has reaped benefits from its recent initiatives. For example, in 2018, countries within Europe improved their Global Cybersecurity Index (GCI) rankings in part because of the implementation of the GDPR and NIS Directive.[56] Higher GCI rankings can improve consumer confidence and promote economic investment, which could prove to be an economically savvy move for Europe.

3.2 The General Data Protection Regulation

Under the GDPR, the protection of personal data is intrinsically linked to technical and organizational security safeguards. Having in place the appropriate safeguards is one of the main ways that companies can avoid or minimize liability in the event of a personal data breach—which, in the case of the GDPR, could result in crippling fines.

3.2.1 Breach Definition

The GDPR defines a personal data breach broadly, addressing leaks, alterations, and denial of access to authorized users.[57] This third prong, in particular, diverges from the definitions common in other jurisdictions, such as the United States. Under Article 4, a personal data breach is "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed[.]"[58] Loss of data is perhaps the most ambiguous category, but the former Article 29 Data Protection Working Party issued guidance to clarify the GDPR's definition.[59] When there has been a "loss" of data, it means that the data "may still exist, but the controller has lost control

[54] Ibid 4.
[55] Ibid.
[56] 'Global Cybersecurity Index 2018' *ITU Publications* (2018) v <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf> accessed 9 May 2019 ("GCI Index 2018").
[57] *See* EU GDPR, Art. 4(12).
[58] Ibid.
[59] Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679 (3 October 2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> accessed 9 May 2019 ("Personal Data Breach Guidelines").

or access to it, or no longer has it in its possession."[60] This category of breach includes data subject to ransomware attacks, a growing threat for organizations storing customers' data.[61]

3.2.2 Appropriateness Standard

Article 32 is the crux of the cybersecurity requirements in the GDPR.[62] Most generally, the GDPR instructs data controllers and processors to adopt "appropriate technical and organisational measures to ensure a level of security appropriate to the risk."[63] Rather than outlining a series of hard-and-fast rules or dictating particular technical requirements, Article 32 transfers the burden of assessing the level of security to the organization processing the data. It outlines several factors that should be considered in determining what is "appropriate"—cost, state-of-the-art technologies, the type of data processing being pursued, and the risk to consumers if the data is compromised.[64] Under this provision, the EU does not expect all companies to adopt state-of-the-art security safeguards. This conclusion is implied by allowing companies to balance costs and risks in making determinations about their security safeguards.

Regulators did, however, give companies an indication of two technical safeguards that are particularly important. Pseudonymization and data encryption are both specifically mentioned in the law, implying that a company would be hard-pressed to justify its safeguards as appropriate without them—even though they are not explicitly required.[65] Furthermore, processors are expected to regularly assess the security safeguards they adopt.[66] The GDPR also emphasizes the importance of incorporating security safeguards into their business design up front.[67] Processes, products, and services should be designed with privacy and security in mind, minimizing the risk to consumers and encouraging innovation in this sphere.[68]

Article 32 outlines no further technical standards, which may make companies intent on minimizing risk uncomfortable. Companies are required to make a broad range of judgment calls, and the consequences of misjudging under the GDPR are severe. A risk mitigation strategy

[60] Personal Data Breach Guidelines, 5.
[61] Ibid.
[62] EU GDPR, Art. 32.
[63] Ibid Art. 32(1).
[64] Ibid.
[65] Ibid Art. 32(1)(a).
[66] Ibid Art. 32(1)(d).
[67] *See* EU GDPR, Art. 25, Rec. 78.
[68] Ibid.

is built in, however. Companies may adopt approved codes of conduct[69] or data protection certifications,[70] increasing the likelihood that they would escape liability in the event of a breach.

3.2.3 Regulator Notification

In general, personal data breaches must be reported to regulators.[71] The GDPR creates an exception for minor breaches, but leaves the determination of whether a breach must be reported to the company. Since the law's presumption is in favor of reporting, a company choosing not to report bears the burden of showing that the breach qualified as an exception.[72] A breach need not be reported if it is "unlikely to result in a risk to the rights and freedoms of natural persons."[73] The exception can crudely filter out the least critical claims for regulators, reducing their workload. The GDPR's penalties and the relatively narrow exception, however, will likely encourage companies to overreport and may still prove a substantial burden.

If regulators conclude that a company's failure to fulfill its regulator notification requirements for a breach demonstrates a shortfall in its security standards more generally, the company could be subject to multiple separate offenses. Each offense can incur a penalty under Article 83.[74] Specifically, WP29 guidance alludes to the possibility of fining a company under Articles 32, 33, and 34 separately based on the same facts.[75]

Prior to the GDPR, many data breaches in Europe activated no notification requirement at all.[76] Now, the GDPR has one of the strictest breach notification timetables in the world. Once a controller is "aware" that its data has been breached, it must notify regulators "without undue delay and, where feasible, not later than 72 hours."[77] Notifying regulators within the designated timeframe is a factor that can aid a company in escaping liability or reducing the penalty imposed under the GDPR.[78] The 72-hour timeframe is a radical change for the cybersecurity industry. A survey of ten years of cyber breach data prior to the GDPR implementation indicated

[69] Ibid Art. 32(3), 40.
[70] Ibid Art. 32(3), 42.
[71] Ibid Art. 33(1).
[72] Ibid Rec. 85.
[73] Ibid Art. 33(1).
[74] Personal Data Breach Guidelines, 8.
[75] Ibid.
[76] Elena Jelmini Cellerini & Christian Lang, 'Cyber Liability: Data Breach in Europe' (July 2018), 85 Def. Couns. J. 1, 3-4.
[77] EU GDPR, Art. 33(1).
[78] Ibid, Rec. 87.

that notification occurred within a 72 hours in a mere 9.1% of cases.[79] It was common for companies to take weeks or months to notify regulators of a large-scale breach.[80] Past performance is not necessarily an indicator of companies' capabilities, however. Drafters of the GDPR were probably aware of the current statistics, but determined that a more aggressive timeline was possible. Critics of this policy argue that the 72-hour rule will generate sloppy, incomplete reports, distract companies from taking emergency steps to reduce harm to consumers, and disadvantage smaller enterprises.[81]

Processors contract with controllers, so their notification obligations are to the controller rather than to a supervisory authority.[82] Once processors determine that a breach has occurred, they must notify the controller "without undue delay."[83] As a risk-management strategy, however, the controller can designate a stricter disclosure policy in its contract with the processor.[84] Such provisions will be likely, as controllers attempt to navigate the 72-hour notification rule and minimize their liability.

Particularly when managing such a short notification timeframe, pinpointing when a company becomes "aware" of a data breach becomes critical. The WP29 guidance explains that a controller is aware when it has "a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised."[85] The guidance does not clarify, however, what level of employee must have knowledge of the breach to constitute awareness. For example, if a low-level employee becomes "aware" of a breach, but fails to communicate it to a superior for a period of time, would the clock start ticking when the first employee was made aware of the issue or when she communicated it to a superior capable of taking action? WP29 only indicates that companies should have a system in place to escalate issues, implying that a breakdown in this process would likely increase the organization's liability.[86] Corporate groups made up of numerous semi-autonomous subsidiaries will struggle to meet the required disclosure timeframes—even if the best internal processes are implemented perfectly, it takes

[79] Allison Davenport, 'CLTC Research: American Companies Struggle to Meet GDPR's Data Breach Notification Rules' *Center for Long-Term Cybersecurity* (16 May 2018) <https://cltc.berkeley.edu/2018/05/16/cltc-research-american-companies-struggle-meet-gdprs-data-breach-notification-rules/> accessed 10 May 2019.
[80] Ibid.
[81] Ibid.
[82] *See* EU GDPR, Art. 33(2).
[83] Ibid.
[84] *See* Personal Data Breach Guidelines, 11.
[85] Personal Data Breach Guidelines, 9.
[86] Ibid 10.

time for security personnel to assess risks and escalate them through a large and complex organization. The guidelines also explain that the controller is considered "aware" of the breach when the processor becomes "aware."[87] Then, not only does the controller have only 72 hours to perform a preliminary investigation and notify the regulator, but it must start the clock before its organization has been notified of the breach.[88]

3.2.4 Customer Notification

In a subset of breaches, a controller is obligated to notify individuals that their personal data was compromised.[89] The controller must determine if the breach is "likely to result in a high risk to the rights and freedoms of natural persons"—if so, it must notify the individuals "without undue delay."[90] Regulators are authorized to mandate that a company notify individuals that their data has been subject to a personal data breach.[91] Companies that invest heavily in cybersecurity, however, may be rewarded for their efforts at this stage. The data subject notification requirement does not apply if data is appropriately protected—particularly if it was encrypted so as to make it "unintelligible."[92] Securely encrypted data for which the company has a copy, ensuring it is still accessible, can also excuse the company from the regulator notification.[93] WP29 makes clear, however, that this determination is not a one-time event—reassessment is necessary to ensure the lost data is not subsequently decrypted.[94]

3.2.5 Penalties

Arguably the most controversial section of the GDPR is its penalties provisions. Most offenses under the GDPR are bifurcated into two categories of penalties. The first category authorizes a fine of up to €10 million or 2% of the organization's total worldwide annual turnover.[95] Failing to notify regulators of a breach in the appropriate time frame is punished under this category. The GDPR has only been in force approximately one year, so data regarding

[87] Personal Data Protection Guidelines, 11.
[88] *See* Ibid 10-11.
[89] EU GDPR, Art 34.
[90] EU GDPR, Art. 34(1).
[91] Arts. 34(4), 58(2)(f).
[92] Art. 34(4).
[93] Personal Data Breach Guidelines, 15-16.
[94] Ibid 16.
[95] EU GDPR, Art. 83(4).

actual fine levels is preliminary. DLA Piper reported, however, that approximately 59,000 personal data breaches were reported in Europe under the GDPR framework from May 2018 to January 2019.[96] The fines imposed so far, however, have been fairly low.[97] The second category permits a maximum €20 million fine or up to 4% of the total worldwide annual turnover.[98] Organizations that process personal data in violation of the GDPR guidelines fall under this fine category.[99] Impermissible conduct includes processing personal data without the "appropriate security safeguards" in place, risking a personal data breach.[100] As intended, the GDPR's penalties shift the risk calculus for companies processing customers' personal data. Failing to meet cybersecurity standards can prompt the imposition of a massive fine that could dramatically undercut the company's bottom line.

4. United States

4.1 The Regulatory Landscape

The United States' approach to data protection and privacy is idiosyncratic, to say the least. Based on a constitution born in an era of colonial resistance, the American conception of privacy is sharply curbed by a strong commitment to a robust, minimally regulated marketplace of ideas. The presence of the world's largest technology companies in the Silicon Valley also drives divergence between the United States and the rest of the world—not only for data protection, but also areas such as competition and hate speech.[101]

Federal regulation in the United States is most often described as "piecemeal"—reactive, industry-specific, and sometimes inconsistent. For example, entities handling healthcare information are governed by the Health Insurance Portability and Accountability Act (HIPAA), while the financial industry is regulated by the Gramm-Leach-Bliley Act (GLBA).[102] Furthermore, the United States' federal system permits states to regulate data protection, privacy,

[96] DLA Piper, 'DLA Piper GDPR Data Breach Survey: February 2019' (2019) 3 <https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/> accessed 10 May 2019.
[97] Ibid.
[98] EU GDPR, Art. 83(5).
[99] Ibid Art. 83(5)(a).
[100] Ibid Art. 5(1)(f).
[101] *See, e.g.,* Sam Schechner, 'Global Regulators Race to Curb Silicon Valley' *The Wall Street Journal* (10 May 2019) <https://www.wsj.com/articles/france-steps-up-global-tech-scrutiny-with-social-media-policing-11557478920?mod=hp_lead_pos4> accessed 10 May 2019.
[102] Martin J. McLaughlin, 'Cybersecurity and the Duty to Protect Client Data' (2018) 91-NOV Wis. Law. 14, 14-15.

and cybersecurity, unless and until they are preempted by the federal government. All states currently have a data breach notification law, in some form.[103] The system is not only incomplete, but also is a complex web of regulations that creates constant frustrations for companies operating across state and national boundaries.

The debate about the future of privacy in America is intensifying, driven in part by European reforms and the 2016 presidential elections. The tech giants are key players in the national, as well as Californian, debates. In 2018, lobbying by the largest tech companies reached new highs: Amazon spent USD $14.2 million; Google, over $21 million; Facebook, $13 million; Microsoft, $5.5 million; and Apple, $6.6 million.[104] The idea of creating a national privacy and data protection law has gained traction.[105] Some experts viewed the passage of a new privacy law in California as a bellweather, predicting a wave of new state legislation across the United States.[106] Others have cautioned that a proliferation of state-dominated legislation will create contradictory standards, hindering business and driving up compliance costs.[107] The tech companies, sensing that the era of self-regulation is coming to an end, appear to be throwing their hat in the ring of national regulation in an attempt to avoid the entrenchment of a complex, fifty-state regulatory scheme.[108]

Focusing on cybersecurity specifically, the United States performs comparatively well against countries around the world. It is considered highly committed to cybersecurity, taking into account five "pillars" of cybersecurity—legal, technical, and organizational measures, in addition to cooperation and investment in capacity building.[109] Surpassed only by the United Kingdom, the United States ranks second in the Global Cybersecurity Index, which measures countries' overall commitment to cybersecurity.[110] Cybersecurity investment in both the public

---

[103] Ibid 15.
[104] Ben Brody, 'Google, Facebook Set 2018 Lobbying Records as Tech Scrutiny Intensifies' *Bloomberg* (23 January 2019) <https://www.bloomberg.com/news/articles/2019-01-22/google-set-2018-lobbying-record-as-washington-techlash-expands> accessed 10 May 2019.
[105] *See* Ryan Tracy & John D. McKinnon, 'Lawmakers Differ on Remedies for Facebook Privacy Breach' *The Wall Street Journal* (8 May 2019) <https://www.wsj.com/articles/lawmakers-differ-on-remedies-for-facebook-privacy-breach-11557343397?mod=article_inline> accessed 10 May 2019.
[106] Forbes Technology Council, 'How Will California's Consumer Privacy Law Impact The Data Privacy Landscape?' *Forbes* (20 August 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#3cb1aff3e922> accessed 10 May 2019.
[107] Ibid.
[108] *See* Brody, supra n. 99 (quoting Noah Theran of The Internet Association, of which Facebook and Google are members: "[The Association is] . . . aligning resources in pursuit of a national privacy law.").
[109] GCI Index 2018, 9, 13.
[110] Ibid 16.

and private sector remains high and continues to grow. For example, in 2018, venture capital funds around the world invested approximately USD $5.3 billion in cybersecurity ventures, about 46% of which were based in the state of California.[111] The Trump administration proposed increasing U.S. government cybersecurity investments to USD $15 billion in fiscal year 2019, a slight increase over the previous year's budget.[112] Like Europe and India, the United States has not been immune to consumer pressures to reform the rules governing cybersecurity, particularly in light of several high-profile breaches in the United States in recent years.[113]

4.2 The California Consumer Privacy Act (CCPA)

State lawmakers passed the California Consumer Privacy Act (CCPA) in 2018 to preempt a proposed ballot initiative resembling Europe's GDPR.[114] CCPA, a milder version of the proposed ballot initiative, is still the most aggressive privacy law in the United States.[115] Although it was enacted in 2018, it is not scheduled to become effective until January 2020.[116] CCPA is grounded in Californians' inalienable right to privacy, written into the California Constitution in 1972.[117] It requires companies to be more transparent with consumers regarding data collection and use and gives consumers some limited rights to control their data's use and transfer to third parties.[118]

CCPA's key cybersecurity innovation is giving consumers a private right of action against organizations that breach their duty of care to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information[.]"[119] This provision

---

[111] Strategic Cyber Ventures, '2018 Cybersecurity Venture Capital Investment' (16 January 2019) <https://scvgroup.net/2018-cybersecurity-venture-capital-investment/> accessed 12 May 2019.
[112] 'Cybersecurity Funding' 273 <https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf> accessed 12 May 2019.
[113] High-profile U.S. data breaches include the Equifax credit monitoring data breach in 2017, impacting 143 million individuals (*see* 'The Equifax Data Breach' *U.S. Federal Trade Commission* <https://www.ftc.gov/equifax-data-breach> accessed 12 May 2019) and the Marriott hotel chain breach in 2018, compromising the data of 500 million customers (Division of Consumer & Business Education, 'The Marriott Data Breach' *U.S. Federal Trade Commission* (4 December 2018) <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> accessed 12 May 2019).
[114] Issy Lapowsky, 'California Unanimously Passes Historic Privacy Bill' *Wired* (28 June 2018) <https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/> accessed 10 May 2019.
[115] *See* Kevin F. Cahill et al., 'California Consumer Privacy Act: Potential Impact and Key Takeaways' (2018) 30 No. 12 IPTLJ 11, 11.
[116] Ibid.
[117] California Consumer Privacy Act of 2018, Assembly Bill No. 375, Cal. Civil Code tit. 1.81.5, § 2(a) (2018) ("CCPA").
[118] CCPA § 2(h)(i).
[119] CCPA § 1798.150(a)(1).

permits a wider latitude of self-determination for consumers, who may bypass regulators and pursue a judicial remedy themselves. Policies such as these can serve as safety valves for overburdened regulators—if the government cannot or will not expend resources to address a certain breach, consumers can still independently take action. Additionally, these provisions are often a way to promote procedural justice; consumers may care more about their day in court and an opportunity to be heard than the actual remedy awarded.

4.2.1 Breach Definition

CCPA implicitly defines a personal data breach in the text of the law. It states: "Any consumer whose nonencrypted or nonredacted personal information[120] . . . is subject to an unauthorized access and exfiltration, theft, or disclosure . . . "[121] The first phrase indicates that companies can escape liability by encrypting or redacting the personal information. The text does not clarify if any level of encryption qualifies, or if a company must achieve a level of certainty that the encryption cannot be broken. The second phrase diverges from the European approach in the GDPR by defining a breach as "unauthorized access, exfiltration, theft, or disclosure"[122] — notably excluding denials of access or corruption of the data.

If the consumer's data is breached according to the criteria above, it still may not qualify for the private right of action. The statute explains that the breach must be a *result* of the company breaching its duty of care with regard to security safeguards.[123] Consequently, companies will not be held to a strict liability standard, but instead the more business-friendly negligence standard.

---

[120] " . . . as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5 . . . " (Ibid): "(A) An individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

(i) Social security number.
(ii) Driver's license number or California identification card number.
(iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
(iv) Medical information.
(v) Health insurance information.

(B) A username or email address in combination with a password or security question and answer that would permit access to an online account." (CAL. CIV. CODE § 1798.81.5(d)(1)(A)-(B) (West 2016)).

[121] CCPA § 1798.150(a)(1).

[122] Ibid.

[123] *See* ibid: " . . . as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action . . . "

4.2.2 Penalties

CCPA's private right of action provision permits consumers to recover actual damages or between USD $100-$750 per person per incident.[124] Consumers may also pursue injunctive relief or "any other relief the court deems proper."[125] This provision seems relatively modest, particularly in comparison to the GDPR's penalties. Given the United States' liberal approach to certifying consumer class actions, however, this provision could prompt enterprising plaintiff attorneys to assemble massive classes against corporate defendants. Such actions could result in crippling penalties, especially for small- or medium-sized companies.[126] Additionally, under this provision, certain types of injunctive relief can be very expensive for companies—sometimes even prohibitively so. The ambiguity of subsections B and C will make it difficult for companies to judge the risk of different compliance approaches and may prompt more investment by risk-averse companies seeking to avoid costly injunctive relief or punitive damages. It may also risk overloading the courts with consumer-initiated litigation.[127]

In addition to consumers' private rights of action, the state Attorney General may bring an enforcement action against a company for a data breach under CCPA. Each CCPA violation carries a maximum fine of USD $7,500.[128] The Attorney General can only pursue this penalty, however, after the state notifies the company of its noncompliance with CCPA and the company fails to cure the violation within thirty days.[129] Unlike the GDPR, CCPA provides companies with a grace period to become compliant and does not tie the penalty to the company's revenues.

4.2.3 Reasonability Standard

Although often compared the GDPR, CCPA regulates a much narrower range of conduct than the GDPR.[130] Its cybersecurity provisions are short and ultimately must be read in

[124] Ibid § 1798.150(a)(1)(A).
[125] Ibid § 1798.150(a)(1)(B)-(C).
[126] *See* David M. Stauss et al., 'Analyzing the California Consumer Privacy Act's Private Right of Action' *Ballard Spahr LLP* (19 November 2018) <https://www.cyberadviserblog.com/2018/11/analyzing-the-california-consumer-privacy-acts-private-right-of-action/> accessed 15 May 2019.
[127] Kristen J. Mathews & Courtney M. Bowman, 'The California Consumer Privacy Act of 2018,' *Proskauer* (13 July 2018) <https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/> accessed 13 May 2019.
[128] CCPA § 1798.155(b).
[129] Ibid § 1798.155(a).
[130] Ibid.

conjunction with another, more specific California cybersecurity law (see Part 4.3).[131] CCPA uses both "reasonable" and "appropriate" to outline the level of security a company is responsible for providing. This standard is in line with most other U.S. states, which generally have adopted reasonability standards.[132] In the absence of case law or additional regulatory guidance from the state of California, companies may choose to look to neighboring states' interpretations of "reasonability" to determine what level of security is needed to achieve compliance with CCPA. Two initial parameters of CCPA's standard are clear at this stage. First, California's standard does not confer an obligation on all companies to implement state-of-the-art security safeguards. Balancing is required to determine what standard is "reasonable." Second, the type of data being processed will influence the type of safeguards a company is expected to implement. In both of these senses, California's law shares several characteristics with Europe's GDPR.

4.3 California Civil Code Sections 1798.81.5 and 1798.82

CCPA must be interpreted in relation to California's breach notification laws, which establish the duty of care companies handling Californians' data must show as well as the notification requirements they incur if they experience a data breach.[133] California implemented both statutes within the last three years.[134] Like CCPA, Section 1798.81.5 establishes a reasonability-based duty of care for security standards:

> A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain *reasonable* security procedures and practices *appropriate* to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.[135]

CCPA's language differs, however, in describing the nature of the breach. Here, both modification and destruction of data, in addition to access, use, and disclosure, can indicate that a data breach occurred.

Next, Section 1798.82 sets out specific notification requirements in the event of a data breach. Interestingly, the Californian approach differs from the European and Indian approaches

---

[131] Cahill, 15.
[132] *See* McLaughlin, 15.
[133] *See* Cal. Civ. Code § 1798.81.5 (West 2016); § 1798.82 (West 2017).
[134] Ibid.
[135] § 1798.81.5(b) (emphasis added).

in its emphasis on consumer notification first, and only in limited circumstances, on regulator notification. Only if a company is required to notify over five hundred Californians of a data breach does it then have an obligation to alert the state Attorney General.[136] Rather than notifying a regulator first, who may require subsequent consumer notification, companies are instructed to directly notify consumers and only involve regulators for larger breaches.[137]

Generally, a security breach is defined as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business."[138] As highlighted in Part 4.2, loss of data is not included in this definition as it is in the GDPR. "Integrity," however, indicates that data corruption would fall under this definition. This law creates an exception for encrypted data—if only encrypted data was stolen and the encryption remains intact, then the company does not incur a notification obligation.[139] If a company experiences a breach, it must notify the impacted California residents in

> the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.[140]

If the law enforcement delay is invoked, the notification must be accomplished "promptly" once law enforcement clears the disclosure.[141] California's law avoids establishing a concrete amount of time for the notification. Instead, it opts for "the most expedient time possible" paired with fairly broad exceptions. This provision gives companies extra time to prioritize remedying the breach and shoring up vulnerabilities in its computer systems before notifying customers of the breach. "Any measures necessary," in particular, delegates a substantial amount of discretion to the company to determine what investigative steps are required and in what order these actions should occur. This choice by the California legislature may be an attempt to avoid exacerbating security breaches further by distracting companies with disclosures. Instead, companies have the freedom to fully understand the problem and create a complete disclosure for customers. It could,

[136] § 1798.82(f).
[137] § 1798.82(a), (f).
[138] § 1798.82(g).
[139] § 1798.82(a).
[140] Ibid.
[141] § 1798.82(c).

however, allow companies to mitigate business risk by delaying disclosures at the expense of customers' privacy.

4.4 Assembly Bill 1130

In addition to CCPA, California's legislature is considering a reform bill to strengthen cybersecurity regulations in the state.[142] Assembly Bill No. 1130 (AB 1130) aims to amend California's existing data breach notification laws, requiring notification for a broader range of data, particularly biometric and passport data.[143] AB 1130 was introduced in February 2019, but is still being discussed in committee.[144] The breach definition and reasonability standard discussed above will not change if AB 1130 is adopted. This bill will only broaden the categories of data that will trigger notification requirements.

Although home to only 39.5 million people, the state of California is the world's fifth largest economy, exceeded only by the United States generally, China, Japan, and Germany.[145] California's market power positions its legislature to influence cybersecurity trends moving forward, particularly since many of the world's largest technology companies are based in Silicon Valley. As the debate about data security, and correspondingly, cybersecurity more generally intensifies in the United States, California's laws will anchor the debate at the national level.

5. India

In general, India's current cybersecurity infrastructure is not strong, but the Indian government has demonstrated a commitment to improving it moving forward. The UN's Global Cybersecurity Index ranked India forty-seventh out of one-hundred seventy-five countries in its commitment to cybersecurity.[146] The report concluded that India demonstrated a high commitment to cybersecurity, placing it in the same category as the United States, the United Kingdom, and Germany.[147] This measure is primarily future-oriented, offering a clearer

[142] Zach Whittaker, 'California to Close Data Breach Notification Loopholes Under New Law' *Tech Crunch* (21 February 2019) <https://techcrunch.com/2019/02/21/california-data-breach-laws/> accessed 13 May 2019.
[143] Ibid.
[144] 2019 CA A.B. 1130 (NS).
[145] Lisa Marie Segarra, 'California's Economy Is Now Bigger Than All of the U.K.' *Fortune* (5 May 2018) <http://fortune.com/2018/05/05/california-fifth-biggest-economy-passes-united-kingdom/> accessed 13 May 2019.
[146] GCI Index 2018, 53.
[147] Ibid 8-9.

perspective on where the country's cybersecurity capability will be in the future given its current prioritization. The ranking is based on, for example, the number of legal institutions, cybersecurity development strategies and training programs, international cooperation agreements, and technological mechanisms to address threats.[148] This ranking is focused on institution-building for cybersecurity, which, while critically important, may not reflect conditions on the ground as accurately. Examining a different ranking focused on more tangible criteria, such as the number of attacks and percentage of computers infected by malware, India did not fare as well.[149] India secured the fifteenth position out of sixty surveyed countries in the world on cybersecurity, with the first spot going to the country with the weakest cybersecurity.[150] The survey reported that a staggering 21.8% of the country's computers were infected with malware, substantially higher than the United States' 10.3%, the UK's 10.5%, and Germany's 15.7%.[151] While India appears to be positioned well for improving its cybersecurity capabilities, cybersecurity threats remain a major risk for companies and the data they store.

5.1 Privacy as a Fundamental Right

Two years ago, the Supreme Court held in *Justice K.S. Puttaswamy (Retd) vs Union of India* that privacy is a fundamental right protected by Article 21 of the Indian Constitution.[152] This decision dramatically altered the status quo of privacy rights in India. Privacy, according to the holding, is a component of an individual's life, personal liberty, dignity.[153] The Indian Supreme Court contrasted its interpretation of privacy from American conceptions under the 4th Amendment by explicitly stating that "privacy is not lost or surrendered merely because the individual is in a public place."[154] One of the most critical components of the *Puttaswamy* decision, for the purposes of this cybersecurity analysis, was the conceptualization of privacy as a positive and negative right. The Supreme Court explained:

> The Constitutional right is placed at a pedestal which embodies both a negative and a positive freedom. The negative freedom protects the individual from

[148] Ibid 3-4.
[149] Rebecca Moody, 'Which countries have the worst (and best) cybersecurity?' *Comparitech* (6 Feb. 2019), <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.> accessed 25 Apr. 2019.
[150] Ibid.
[151] Ibid.
[152] *Justice K.S. Puttaswamy (Retd) v. Union of India*, (2017) Writ Petition (Civil) No. 494 of 2012 (India), 262.
[153] Ibid.
[154] Ibid 263.

> unwanted intrusion. As a positive freedom, it obliges the State to adopt suitable measures for protecting individual privacy.[155]

Interpreting privacy negatively is a narrower conception of the right. Imposing an affirmative obligation, however, creates much more ambiguity around the government's duty to protect Indian citizens' privacy. Does the government's duty cover only data stored by government agencies, or does it extend to the private sector as well? What level of security is "suitable?" This decision was the main impetus behind the drafting of India's proposed Personal Data Protection Bill (PDPB).[156] The judgment itself called on the government to "implement a robust regime for data protection" in India, balancing the government's compelling interests against individual privacy concerns.[157]

5.2 THE PRE-PDPB LANDSCAPE

The PDPB would likely displace India's older and industry- or program-specific cybersecurity laws. For example, the Aadhaar Act of 2016 included cybersecurity provisions governing government agencies and private sector partners handling data relating to Aadhaar, India's nationwide biometric identification program.[158] Indian residents' data will be stored centrally in a government-run database called the Central Identities Data Repository (CIDR).[159] Additionally, during enrollment into the Aadhaar program and each subsequent authentication of a user's identity, government partners will process users' personal data. Partners can include private companies, such as banks and telecom providers, non-profit organizations, administrative agencies, and state governments. The security of the computer systems storing and processing such data is critical to the protection of users' data. Section 28 is the key cybersecurity provision, outlining a combination of technical and organizational standards. Formal analysis of this

---

[155] Ibid 222.
[156] D. Reed Freeman & Meghan Koushik, 'India Considers Stringent New Personal Data Privacy Law,' *WilmerHale* (3 Aug. 2018) < https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20180803-india-considers-stringent-new-personal-data-privacy-law>. *See* The Personal Data Protection Bill, MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY (2018), https://meity.gov.in/content/personal-data-protection-bill-2018 (India).
[157] *Puttaswamy* (2017) (India), 264-65.
[158] Aadhaar Act, §§ 28-33.
[159] Pavan Duggal & Rashi Varshney, 'India's Aadhaar Law and Cyber Security, With A Legal Eye,' Express Computer (2 May 2016) <https://www.expresscomputer.in/columns/indias-aadhaar-law-and-cyber-security-with-a-legal-eye/17347/> accessed 27 Apr. 2019.

provision is minimal in the Indian courts or administrative agencies. Subsection (1), if read in isolation, appears to establish a stringent standard by opting to use the word "ensure":

> "(1) The Authority shall ensure the security of identity information and authentication records of individuals."[160]

In combination with subsequent provisions, which outline more specific mandates for the government, however, subsection (1) is more likely intended to be read as a purposive provision. The operative standard is established in subsection 4:

> (4) Without prejudice to sub-sections (1) and (2), the Authority shall—
>
> (a) adopt and implement *appropriate* technical and organisational security measures;
>
> (b) ensure that the agencies, consultants, advisors or other persons appointed or engaged for performing any function of the Authority under this Act, have in place *appropriate* technical and organisational security measures for the information; and
>
> (c) ensure that the agreements or arrangements entered into with such agencies, consultants, advisors or other persons, impose obligations equivalent to those imposed on the Authority under this Act, and require such agencies, consultants, advisors and other persons to act only on instructions from the Authority.[161]

Appropriate, like reasonable, is a standard that requires balancing between the nature of the data and the risk of a cyber incident. On its face, this standard offers little reassurance for skeptics of the Aadhaar program who fear that the data will be compromised or misused. It also offers very little in terms of implementable guidelines for organizations involved in Aadhaar. India's IT Acts, discussed below, may influence the interpretation of this standard—in particular, reinforcing its proportionality judgment. The CIDR database has been designated critical infrastructure by the Indian government.[162] Correspondingly, additional guidelines were promulgated to mandate more specific cybersecurity measures, including creating a Cyber Crisis Management Plan and coordinating with the National Critical Information Infrastructure Protection Centre.[163]

---

[160] Aadhaar Act § 28(1).
[161] Ibid § 28(4).
[162] Ministry of Communications and Information Technology (Department of Electronic and Information Technology) Notification, THE GAZETTE OF INDIA EXTRAORDINARY (11 Dec. 2015), <https://www.meity.gov.in/writereaddata/files/UIDAI%20CII%20notification%20Dec15.pdf> accessed 27 Apr. 2019.
[163] *See* Ministry of Electronics and Information Technology Notification, The Gazette of India Extraordinary (22 May 2018), <https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf> accessed 27 Apr. 2019.

Additionally, India's Information Technology Act (IT Act) was implemented in 2000 and revised in 2008.[164] The 2000 IT Act codified several common cyber crimes, such as altering a computer's source code,[165] hacking,[166] and publishing obscene material,[167] but lacked strong data protection standards. One section of the law made it a criminal offense, punishable by a fine or prison sentence, to gain access to electronic information and disclose it without the consent of the affected individual.[168]

The amended 2008 law introduced a cybersecurity standard for corporations handling sensitive personal information. Specifically, it allows individuals to sue if a company handling their sensitive or electronic data "is negligent in implementing and maintaining reasonable security practices."[169] The law leaves substantial latitude in interpreting "reasonable security practices," including practices dictated by a contract between parties sharing data, another more specific law (if it exists), or the Central Government's guidance.[170] In addition, the 2008 IT Act made it a criminal offense, punishable by a fine or jail time, for a person to disclose personal information under a contract without the consent of the impacted individual.[171] The action requires a mens rea of intentionality or knowledge.[172]

The most informative standards for companies navigating Indian cyberlaw are rules promulgated by the Central Government under the authority of the two IT Acts. Specifically, the government's 2011 rules outline in more concrete terms the meaning of "reasonable" cybersecurity measures.[173] Corporations must create a cybersecurity plan that is "commensurate with the information assets being protected."[174] This is a proportionality standard that puts the

---

[164] 'Information Technology Act,' Ministry of Electronics & Information Technology (24 Aug. 2016) <https://www.meity.gov.in/content/information-technology-act> accessed 25 Apr. 2019.
[165] The Information Technology Act, 2000, No. 21 of 2000, THE GAZETTE OF INDIA EXTRAORDINARY (2000), § 65, <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf> accessed 27 Apr. 2019 (IT Act, 2000).
[166] Ibid § 66.
[167] Ibid § 67.
[168] *See* ibid § 72.
[169] The Information Technology (Amendment) Act, 2008, No. 10 of 2009, THE GAZETTE OF INDIA EXTRAORDINARY (2009), § 43A <https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf> accessed 27 Apr. 2019 ("IT Act, 2008 Amendment").
[170] Ibid.
[171] Ibid § 72A.
[172] Ibid.
[173] Ministry of Communications and Information Technology (Department of Information Technology) Notification, G.S.R. 313(E), The Gazette of India Extraordinary (2011), ¶ 8, <https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf> accessed 27 Apr. 2019 (G.S.R. 313(E) Notification).
[174] Ibid ¶ 8(1).

burden on corporations to assess the nature of the data they store and process, their business, and the risk for their customers. If a corporation's systems are breached, it is responsible for proving that its practices adhered to its security plan in order to avoid liability.[175] A corporation can implement international cybersecurity standards, which, if adhered to, can absolve it of liability in the event of a breach.[176]

5.3 The Proposed Personal Data Protection Bill (PDPB)

A committee of experts, led by a former Supreme Court justice, convened following the 2017 decision to assess India's data protection needs and draft a comprehensive data protection bill.[177] The resulting bill was publicly released in July 2018, but has not yet been formally proposed in the legislature.[178] Drafters are expected to submit a revised version of the bill to the legislature in June 2019, following India's national elections.[179] In many ways, the PDPB is modeled off of the GDPR, incorporating nearly identical language from its European counterpart. Since the PDPB has not been enacted into law, there are very few signposts from Indian regulators indicating how its provisions should be interpreted. This analysis offers preliminary interpretations based heavily on the PDPB's text.

---

[175] Ibid.
[176] Ibid ¶ 8(1)-(3). *See also* S.S. Rana & Co., 'India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,' *Lexology* (4 Sept. 2017), <https://www.lexology.com/library/detail.aspx?g=35f56a2a-c77c-49e7-9b10-1ce085d981dd> accessed 27 Apr. 2019.
[177] Surabhi Agarwal, 'Justice BN Srikrishna to head Committee for data protection framework,' *The Economic Times* (New Delhi 1 Aug. 2017) <https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection-framework/articleshow/59866006.cms> accessed 25 Apr. 2019.
[178] Kurt Wimmer, 'India's Committee of Experts Releases Draft Personal Data Protection Bill,' *Covington & Burling LLP* (30 July 2019) <https://www.insideprivacy.com/international/indias-committee-of-experts-releases-draft-personal-data-protection-bill/> accessed 25 Apr. 2019.
[179] *See* Surabhi Agarwal, 'Personal Data Protection Bill only after new government takes over,' *The Economic Times* (New Delhi 4 Jan. 2019) <https://economictimes.indiatimes.com/tech/internet/personal-data-protection-bill-only-after-new-government-takes-over/articleshow/67374919.cms> accessed 25 Apr. 2019.

5.3.1 Appropriateness Standard

The PDPB's Article 31 outlines the security requirements for data fiduciaries[180] and processors.[181,182] The central component of the PDPB's security guidance is that "the data fiduciary and the data processor shall implement appropriate security safeguards."[183] The provision offers only minimal guidance on how an organization should determine what security measures are "appropriate." It instructs the fiduciary or processor to consider several factors, including the type of processing, the risks such processing entails, and the consequences of a breach of that data.[184] These considerations are malleable and judgment-laden, providing little security to an organization attempting to ensure that their data systems are in compliance. Interestingly, this provision does not explicitly include a consideration of costs. It does not ask companies to use state-of-the-art measures, but also does not give them a clear prerogative to invest in security measures that make economic sense. It only asks them to weight the consequences to the data. A cost consideration may be implied in the word "appropriate," but it would more feasibly be interpreted as a deliberate omission. If any economic security options would be insufficient to safeguard the data in light of the potential consequences of a breach, the organization may be expected to forego that processing altogether.

Following the general security standard, Article 31 outlines a series of disjointed "security safeguards" that organizations must put in place in conjunction with their data processing operations. First, companies are required to implement "methods such as de-identification and encryption."[185] This subsection does not clarify whether this is a universal requirement or dependent on the nature and risk of the organization's data processing. The implication, however, is that a company lacking these two security measures would be likely held liable in the event of a data breach. Second, the organization must take "steps necessary to protect the integrity of personal data."[186] And third, it must take "steps necessary to prevent misuse,

[180] Data fiduciary is defined as "any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data." PDPB, Art. 3(13).
[181] Data processor is defined as "any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary." PDPB, Art. 13(15).
[182] *See* PDPB, Art. 31.
[183] Ibid Art. 31(1).
[184] Ibid.
[185] Ibid Art. 31(1)(a).
[186] Ibid Art. 31(1)(b).

unauthorised access to, modification, disclosure or destruction of personal data."[187] These two requirements modify the general appropriateness standard. While vague and open to a wide latitude of interpretations, both could be construed to strengthen the standard of security. While unlikely, they could be used to imply a strict liability standard—a data breach compromising the integrity of users' personal data did not possess the security measures necessary to prevent such an outcome. It is more probable that if adopted, this provision would be interpreted as a reasonability standard, permitting organizations to balance the processing risks and available technologies.

Finally, this article makes clear that the assessment of security safeguards is not a one-time exercise. Organizations are required to reevaluate their security measures "periodically as may be specified."[188] Regulations clarifying this language would be promulgated only after the PDPB is passed.

5.3.2 Notification Requirements

Article 32 addresses an organization's requirements following a personal data breach,[189] including notification to Indian regulators, disclosure to individuals whose data has been breached, and actions to remedy the damage.[190] The PDPB's notification provision is extremely broad, requiring notification of "*any* personal data breach . . . where such breach is likely to cause harm to any data principal."[191] Read literally, this provision would open the floodgates for Indian regulators, who would have to sift through data breach notifications from one erroneously sent email implicating the data of a single person to large-scale breaches compromising millions of individuals' data. Particularly in a country the size of India, this notification provision could generate an unworkable system of government breach response.

One of the most critical data breach regulation choices is determining the timetable dictating how quickly an organization must notify regulators of a cyber incident, once it is discovered. Here, the PDPB allows the clock to start ticking for organizations after they have taken

[187] Ibid Art. 31(1)(c).
[188] Ibid Art. 31(2).
[189] "'Personal data breach' means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal[.]" Ibid Art. 3(30).
[190] Ibid Art. 32.
[191] Ibid Art. 32(1).

emergency measures to address the breach (e.g., to stem the flow of outgoing data).[192] This mitigates the risk that the law will exacerbate the effects of a breach—for example, incentivizing a company to prioritize government disclosure over preventing further harm to consumers' privacy. After such emergency measures have been implemented, the notification timeline begins. The provision punts to regulators, saying that notifications should occur "as soon as possible and not later than the time period specified by the Authority."[193]

Notably, the PDPB avoids using a strict hour or day timeline for reporting breaches. This was not an accidental omission; the committee considered the GDPR's 72-hour timeline in its 2017 white paper, expressing skepticism that such a strict notification timeline would be beneficial for companies with many subsidiaries or small- and medium-sized enterprises without large-scale cybersecurity operations.[194] Instead, the committee seemed more convinced by two U.S. state-level approaches, which often require notification "as soon as possible" and "in the most expedient time possible," but which also sometimes include a cap of 45 days.[195] The current PDPB draft does not include such a cap, but the white paper indicates that it may be a serious consideration for future iterations.

Indian regulators will make the determination of what measures must be taken to address the breach and whether the individuals whose data was compromised must be notified of the breach.[196] Regulators have also reserved the right to require the organization to publicly post notification of the breach and post it on government websites.[197] Considering the floodgates concern presented by a literal reading of Article 32(1), these provisions may prove problematic for individuals. If the government is overwhelmed with screening minor breach notifications, it may not have the capacity to promptly instruct organizations on next steps. What steps those organizations must take in the absence of government input is not explained in the PDPB.

---

[192] *See* ibid Art. 32(3).
[193] Ibid.
[194] *See* Justice B.N. Srikrishna et al., 'White Paper of the Committee of Experts on a Data Protection Framework for India,' (2017) Ministry of Electronics and Information Technology (MeitY), 163-64 <https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf> accessed 8 May 2019 ("Committee of Experts White Paper").
[195] Ibid, 164.
[196] PDPB Art. 32(5).
[197] Ibid Art. 32(6)-(7).

5.3.3 Penalties

The PDPB's penalty regime is a near carbon copy of Europe's GDPR. Most offenses are segmented into two main penalty categories. The first category triggers a maximum fine of five crore rupees (approximately USD $715,000) or two percent of an organization's total worldwide turnover.[198] This penalty can be administered if an organization fails to adequately respond to a data breach.[199] The second category permits a maximum fine of fifteen crore rupees (approximately USD $2.1 million) or four percent of an organization's total worldwide turnover.[200] This penalty applies to an organization that falls short of the security safeguards required by Article 31.[201] Like the GDPR, these penalties apply to the global revenue generated by the entire corporate group.[202] They are penalties intended to intimidate the world's largest tech companies, such as Google, Facebook, and Twitter, into compliance. Unlike the GDPR, however, the security provisions that the penalties are based on are, at least at this stage, less clear and developed. Determining how much investment is needed to avoid crippling fines will be a critical challenge for companies operating in India if the PDPB is adopted.

6. Comparing Approaches

6.1 Breach Definition

In general, U.S. definitions of a personal data breach are more restrictive than either the EU's GDPR or India's PDPB definitions.[203] In particular, the EU and Indian approaches expand the definition beyond unauthorized disclosure or alteration of the data to include restrictions of access to the data.[204] The prevalence of ransomware attacks may be driving India and Europe's choice to expand the definition. A 2019 report explained that ransomware constitutes 24% of malware-based cyber incidents.[205] Denying a legitimate user access to their information can

[198] Ibid Art. 69(1).
[199] Ibid Art. 69(1)(a).
[200] Ibid Art. 69(2).
[201] Ibid Art. 69(2)(e).
[202] Ibid Art. 69.
[203] *See* Justice B.N. Srikrishna et al., 'White Paper of the Committee of Experts on a Data Protection Framework for India,' (2017) Ministry of Electronics and Information Technology (MeitY), 161-62 <https://innovate.mygov.in/wp-content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf> accessed 8 May 2019.
[204] Ibid.
[205] Verizon, '2019 Data Breach Investigations Report' (May 2019) 3 <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf> accessed 13 May 2019.

cause them substantial harm—for example, if healthcare data is maliciously encrypted and held for ransom, the physical health of the effected person can be compromised. One challenge with defining a breach as a denial of access is determining the timeframe required for it to become a breach. Specifically, was the data breached if it was held for ransom temporarily, but access was restored after a short period of time? WP29 specifically addresses this issue for Europe's GDPR, explaining that a temporary loss of access is a data breach, but the controller must evaluate whether it needs to be disclosed on case-by-case basis.[206] The central consideration is whether the temporary access denial could risk data subjects' rights and freedoms.[207] The nature of the data will impact the analysis; for example, healthcare data would be more likely to require disclosure than commercial data.[208]

In the United States, hackers have disproportionately targeted the healthcare industry for ransomware attacks, resulting in several high-profile ransoms of major hospitals in recent years.[209] Hackers appear to be taking advantage of hospitals' comparatively poor cybersecurity and recent U.S. efforts to digitize health records to improve health outcomes.[210] As hospitals dealt with a slew of ransomware attacks, prior to 2016 there was an open question of whether hospitals had to report a "breach" when a hacker temporarily ransomed patient data, but subsequently released it when the hospital paid the demanded amount. The Department of Health and Human Services (HHS), a national agency overseeing the healthcare industry, finally clarified in 2016 that such events were presumed by the government to be a breach triggering a notification requirement, unless the hospital could prove that it was unlikely that the hacker compromised the data.[211] While this U.S. agency opted to adjust its interpretation of a "breach," failing to write it into state and federal statutes in the United States will continue to generate confusion for regulators and companies confronting ransomware attacks. California's choice to omit language similar to the GDPR including data loss in the definition of the breach is no exception.

[206] Personal Data Breach Guidelines, 7.
[207] Ibid.
[208] Ibid.
[209] Connor McLarren, 'Once More Unto the Breach: How the Growing Threat of Ransomware Affects HIPAA Compliance for Covered Entities' (2018) 15 Ind. Health L. Rev. 305, 312-14.
[210] Ibid, 307-08.
[211] Ibid.

The United States should adopt the European and Indian approach to defining a data breach by explicitly including "loss of access" as a component of a breach. To adequately protect data, cybersecurity laws must adapt to accommodate the evolving threat landscape. The rise of ransomware attacks has challenged traditional American conceptions of a cybersecurity incident and generated confusion when the laws have not been clear on that point. However, the committee of experts in India was correct when it noted that "determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious."[212] If not carefully cabined, including availability in the definition of breach can prompt a wave of notifications that may overwhelm regulators and divert resources from more serious cyber attacks. When jurisdictions adopt this principle, therefore, they should limit it by tying it to a harm principle, as the EU does. If there is little or no risk of harm to the data subjects, then companies should be under no obligation to report the breach.

There was general agreement between the Californian, Indian, and European approaches on the importance of data encryption. In CCPA and the GDPR, uncompromised encryption of stolen data was written in as an exception to the breach notification laws.[213] India, while emphasizing the importance of encryption, did not explicitly exempt encrypted data from its breach notification requirements, but rather listed encryption as an example of an appropriate security safeguard.[214] Under the PDPB, companies must report a breach when "where such breach is likely to cause harm to any data principal."[215] Tying notification to a harm principle may be a way to implicitly create an encryption exception—if uncompromised encrypted data is stolen, then the harm to consumers is minimal and a company can avoid the obligation to report.

New laws implementing data security standards should create an encryption exception, which will align the interests of companies, regulators, and customers. It will create a strong incentive for companies to encrypt their data to avoid costly disclosures altogether, preemptively reducing the risk that customers' data will be compromised. While notification is important for customers, the best laws will prevent their data from being accessed by unauthorized parties in the first place. Encryption is not a panacea, however, so this exception should be subject to a periodic reevaluation requirement to ensure that even if the data remains securely encrypted when it is

[212] Committee of Experts White Paper, 161.
[213] *See* EU GDPR, Art. 34(3)(a); § 1798.82(a).
[214] *See* PDPB, Art. 31(1)(a).
[215] PDPB, Art. 32(1).

stolen, it is not subsequently decrypted. Companies should be required to periodically reassess the security of that data, and if they reasonably believe that it has been decrypted, they must notify regulators or individuals of the breach. This approach is most in line with the GDPR, which holds companies accountable for assessing the ongoing security of stolen encrypted data.[216]

6.2 Security Standards

India's PDPB and the EU's GDPR put in place similar security standards; the PDPB requires "appropriate security safeguards"[217] while the GDPR calls for "appropriate technical and organisational measures."[218] The CCPA, varying only slightly, requires companies to put in place "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."[219] All three jurisdictions opted for a standard, rather than specific rules that would quickly become outdated. Additionally, these standards are essentially balancing tests, requiring companies to assess the data that they are processing and determine themselves which security measures would sufficiently mitigate the risks of a breach. Tech companies, in particular, are leading the world in cybersecurity capability. They almost certainly outpace the government's capability in many areas. As a result, crafting a standard that places the burden on these companies to identify necessary technology practices is an effective use of resources. It promotes innovation for companies seeking to mitigate the risk of a breach, shifts the burden of identifying specific security techniques from the government to regulated entities, and ensures that the law will not quickly become outdated as threats evolve.

Appropriateness or reasonability standards have drawbacks, however. Under these standards, most companies will not have an obligation to implement state-of-the-art security solutions. Instead, they are incentivized to implement an average level of security for the type of data they are processing. As a result, companies may become complacent once they have reached an acceptable level of security, even if they have the capability to develop more sophisticated security solutions. This standard also does not give companies a clear path to compliance. As a result, highly risk-averse companies will invest a socially inefficient amount in security, while

[216] Personal Data Breach Guidelines, 16.
[217] PBPD, Art. 31(1).
[218] GDPR, Art. 32(1).
[219] CCPA § 1798.150(a)(1).

others will misjudge and underinvest, resulting in avoidable data breaches. While this is a challenge, it is unlikely that regulators could issue more prescriptive rules in a more timely, targeted way than the companies themselves.

The GDPR and PDPB outlined several factors that must be considered to determine what security safeguards will fulfill companies' obligations. The GDPR instructs companies to assess state-of-the-art technologies and practices, costs, the data being processed, and the risk of harm to consumers if there were a breach.[220] By contrast, the PDPB instructs companies to consider the data processing, risk, and "likelihood and severity of the harm" to consumers.[221] Cost and state-of-the-art are conspicuously absent from India's list. While the latter may reasonably be implied in any consideration of balancing, failing to include cost as a factor was likely deliberate. Interestingly, however, India's Committee of Experts explicitly acknowledged the importance of considering the costs of companies' security safeguards.[222] No justification is provided for its apparent reversal in the PDPB draft—this is one area that may change in the new June 2019 draft to accommodate India's business interests. CCPA was silent on costs, but also avoided enumerating factors altogether. Since U.S.-based approaches are typically more liberal with regard to consumer privacy and more strongly weight business interests, in practice, costs would be almost certainly a permissive consideration.

In determining the appropriate policy, legislators and regulators must consider two competing harms to consumers. First, that some companies may be driven out of business or be unable to invest in new products and technologies if data security costs are too high. In particular, a policy that ignores the burden of costly security safeguards may risk entrenching large, existing players in the market by creating a high barrier to entry for smaller start-ups. The cost factor allows smaller companies to implement weaker security safeguards, given their limited resources, without forcing them to abandon data processing. Second, if costs are a factor, some companies may engage in high-risk processing with inadequate security safeguards because the costs would be crippling to the business. As a result, consumer data may be put at risk by small- and medium-sized enterprises engaged in a socially inefficient level of data processing. For a consumer whose data was breached, it does not matter whether a resource-poor

[220] EU GDPR, Art. 32(1).
[221] PDPB, Art. 31(1).
[222] Committee of Experts White Paper, 150.

or resource-rich company failed to protect the data; it matters that the consumer's privacy is compromised.

Taking into account these considerations, the approach that strikes the best balance for consumers' interest is a reasonability security standard that considers cost factors. Either in the law or subsequent regulations, the government should make clear, however, that cost considerations cannot overwhelm other factors. Reasonability should entail obtaining a baseline level of security for the type of data being processed; if that cannot be done in a cost-effective way for the business, then that business must reformulate its product or service offerings. A major drawback of this approach is a lack of up-front clarity. Furthermore, well-crafted regulations can help to mitigate wasteful compliance spending that is a result of murky standards.

While the laws analyzed above generally avoided making prescriptive technical rules, both the GDPR and the PDPB emphasized the importance of encryption and pseudonymization above other measures.[223] The Article 29 Working Party explained that proper encryption is a "reasonable guarantee" of online data's security.[224] Industry experts also herald encryption as the key mechanism to safeguard data.[225] The value of including an encryption exception and stressing the importance of encryption to appropriate security safeguards specifically seems clear. By creating large benefits for encrypting data, namely excepting encrypted data from the definition of a breach and / or excusing companies from notification if the data stolen was appropriately encrypted, legislatures change the cost-benefit analysis companies face when developing security policies. Calling out this technical safeguard can also reduce oversight costs—by creating what is akin to a de facto rule, regulators can more quickly parse the more reckless companies and higher-risk breaches that require more government attention.

By contrast, pseudonymization and de-identification strategies have been much more heavily critiqued in recent years. While the overall impact of such safeguards are still positive, they are not guarantees of consumers' privacy. For example, Australian researchers were able to re-

---

[223] *See* EU GDPR, Art. 32(1)(a); PDPB, Art. 31(1)(a).
[224] Article 29 Working Party, 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU' *IAPP* (11 April 2018) <https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionePrivacypdf%20(1).pdf > accessed 16 May 2019.
[225] *See, e.g.,* Kurt Rohloff, 'Why Encryption Holds the Secret to Data Security,' *TDWI* (29 March 2019) <https://tdwi.org/articles/2019/03/29/dwt-all-why-encryption-holds-the-secret-to-data-security.aspx> accessed 16 May 2019.

identify patients in a de-identified healthcare dataset using publicly available data, calling into question companies' and regulators' confidence in de-identification techniques.[226] Considering its drawbacks, should provisions like Section 1798.145(a)(5) of CCPA, which excuses de-identified information from CCPA's data restrictions, be eliminated?[227] Similarly, under the GDPR, while pseudonymized data is considered personal data, anonymized data is not.[228] Even anonymization, which is generally considered more secure than pseudonymization, is not irreversible.[229] While there are risks, the GDPR and California made the right determination by offering substantial benefits for pseudonymization to encourage its adoption, but maintaining limits on the exception. For example, to qualify as de-identification in the first place, the CCPA requires that the data have in place "technical safeguards that prohibit reidentification."[230] In one sense, this decision risks creating circular logic in the data protection laws. Pseudonymization is an indication of stronger security safeguards, but reversible pseudonymization fails to meet the requirements. This approach is practical, however, because it shifts the technical determination onto the most technologically sophisticated party—the company.

6.3 Notification Timetables and Requirements

There are two general categories of notification requirements—regulator and consumer notification. The GDPR adopts by far the most aggressive timetable for regulator notification of the three jurisdictions. It is the only law of the three analyzed that sets of a concrete, hours-based timetable. By contrast, California opted for a standard rather than an unyielding hours limit, requiring consumer notification in "the most expedient time possible and without unreasonable delay."[231] California's approach is more common in the United States, where a select number of states have implemented a notification deadline of thirty or forty-five days, but most have remained with the more subjective "without unreasonable delay" standard.[232]

---

[226] *See* Chris Culnane et al., 'Health Data in an Open World,' (15 December 2017) arXiv:1712.05627 <https://arxiv.org/abs/1712.05627> accessed 16 May 2019.
[227] CCPA § 1798.145(a)(1).
[228] *See* Laura Jehl & Alan Friel, 'CCPA and GDPR Comparison Chart, Baker & Hostetler LLP (2018) 2 <https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf> accessed 16 May 2019.
[229] *See* Committee if Experts White Paper, 37.
[230] CCPA § 1798.140(h)(1).
[231] § 1798.82(a).
[232] Caleb Skeath & Brooke Kahn, 'State Data Breach Notification Laws: 2018 In Review' *Covington & Burling LLP* (31 December 2018) <https://www.insideprivacy.com/data-security/data-breaches/state-data-breach-notification-laws-2018-in-review/> accessed 15 May 2019.

India's approach differs from both the European Union and California. The PDPB notification timetable is delegated to regulators,[233] but as discussed above, drafters seemed more convinced by the American rather than European approach. A standard-based approach is the most likely outcome for India.

Each jurisdiction offers a slightly different version of the urgency exception, delays the start of the notification clock until after companies have taken immediate steps to mitigate the damage of the breach. India's notification timetable starts "after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm."[234] California's without unreasonable delay standard begins after it is determined that the notification will not interfere with an investigation by law enforcement.[235] Furthermore, companies can first take "any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system."[236] Absent clarifying interpretations from the courts or regulators, California's standard appears to be the more liberal of the two. It permits companies to determine the scope of the breach prior to notification, whereas the Indian standard allows companies to address the harm posed to customers. Furthermore, under the Indian bill, companies can only address immediate harms, while companies under the California statute can work to reestablish the system's integrity, limited by the word "reasonable."

Unsurprisingly, the GDPR creates the least permissive exception for urgent actions. If a company misses the 72-hour deadline, they may submit an explanation with their notification to a regulator explaining the reason for the breach.[237] Although not written into the statute, this provision implies that an explanation based on the foundational principles of the GDPR—e.g., protecting consumers' data privacy—may serve as a mitigating factor for regulators making enforcement or penalty decisions.[238]

Here, the Indian approach is most practical to achieve balance between rapid disclosure to regulators and safeguarding consumer data that may be actively under threat when the data breach is discovered. Without a robust urgent action exception, the rule itself can threaten consumers' privacy. If companies are incentivized to disclose to avoid liability before mitigating

[233] PDPB, Art. 32(3).
[234] PDPB, Art. 32(3).
[235] § 1798.82(a).
[236] Ibid.
[237] EU GDPR, Art. 33(4).
[238] Ibid Art. 33(1).

reasonable harms, the rule undermines its own purpose. The PDPB, in allowing companies to address "immediate" harms, rewards companies for taking action to protect consumer data, without giving them broad outs to complete investigations while keeping regulators in the dark.

The three jurisdictions also disagreed regarding the circumstances in which a company must notify its regulator of a data breach. California created a stronger gatekeeping function to reduce the number of notifications to its state Attorney General. In California, must only notify the Attorney General if greater than five hundred customers were impacted by the breach.[239] This approach is consistent with several other U.S. states, including Colorado and Arizona.[240] A major benefit of such a baseline requirement is to avoid overwhelming Attorneys General, who often have very limited budgets and small staffs. Government time and attention should be focused on addressing the most egregious breaches. The private right of action provision also offers plaintiffs an avenue to hold companies accountable for data breaches, without straining state budgets further.

Rather than creating a threshold based on number of customers impacted, the GDPR and India opted for a standard-based system. Under the GDPR, companies must report the breach unless it "is unlikely to result in a risk to the rights and freedoms of natural persons."[241] Similarly, India requires notification if the breach is "likely to cause harm to any data principal."[242] Presumably, most breaches would risk some harm to a data subject, unless thorough pseudonymization or encryption were in place. These exceptions will not screen out a large number of cases, but it will keep the most benign breaches off of regulators' radars—allowing them to focus attention and government resources on more critical breaches.

When determining which version to adopt, one key question is which of these or other alternative approaches strikes the right balance to ensure that critical breaches will be reported and addressed by regulators, while avoiding significant backlogs and wasteful government spending as governments attempt to triage large numbers of notifications? Relatedly, should the line be drawn using the number of consumers or a version of a harm principle? Addressing the first question, whether the harm principle is an effective filtering mechanism should be evaluated on a country-by-country basis, given the efficiency of government regulators and the risk

[239] § 1798.82(f).
[240] *See* Caleb Skeath & Brooke Kahn, 'State Data Breach Notification Laws: 2018 In Review.'
[241] EU GDPR, Art. 33(1).
[242] PDPB, Art 32(1).

aversion of companies operating in that space. One benefit of these disparate approaches across the world is the opportunity to compare outcomes over the next several years. I predict that given high penalties in Europe and India, companies will overreport to regulators, who will be unable to maintain large enough staffs with the appropriate expertise to triage notifications. Consequently, enforcement may be spotty and other functions that those regulators could serve—coordinating between Member States or provinces, for example, will be impeded.

Regarding the second question, categorizing data breaches by degree of harm rather than number of customers more closely aligns the rule to the purpose it is supposed to serve. Each customer's rights is valuable; while flagging large-scale breaches can be a useful mechanism, ultimately it is a crude one. A harm principle is less clear-cut for companies, which will increase compliance costs. It requires an internal judgment call regarding whether or not to report. But it also will allow regulators to identify particularly egregious practices while they only impact a smaller number of customers, before they grow into much larger problems.

The answers to these two questions point in different directions—the simplicity of a customer count-based approach is appealing for resource-strapped government agencies, while the harm principle is a better fit to accomplish the goals of data privacy and protection regulations. Consequently, in the short term before more empirical data is collected, countries with more government resources and deeper human capital expertise in this area should opt for the harm principle, despite the risk of overwhelming government agencies. This recommendation should be revisited in the future, however.

Customer notification provisions are another area where the three jurisdictions diverge in their approaches. In California, customer notification seems to supersede regulator notifications. While regulator notifications are strictly limited, as discussed above, the presumption is in favor of consumer notification.[243] In India, however, companies must go through government regulators first, who then may instruct them to notify regulators.[244] Finally, under the GDPR, consumers must be automatically notified if the possible harm they will incur from the breach is

[243] § 1798.82(a), (f).
[244] *See* PDPB, Art. 32(5): "Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm."

severe enough.[245] Consumers are not notified of every breach, but nor is their notification dependent on government action.

One key concern in designing these regulations is the possibility that government agencies will become backlogged, given the large number of cyber incidents that take place and stringent penalties on companies for nondisclosure. The Indian approach, which requires the most government involvement, risks consumers' privacy by having companies go first through the government before informing consumers. The Californian approach, which prioritizes the consumer over regulator notification, is favorable to the PDPB's. Regulators will also be notified under Californian law, but consumer notification is not contingent on approval from possibly overburdened regulators. Consumers receiving too many notifications may become overwhelmed by companies' disclosures and become desensitized. The GDPR approach, therefore, strikes the right balance between limiting consumer notifications to the breaches that most risk their privacy, while avoiding government approvals before the notification can be issued.

6.4 Penalties

Unsurprisingly, the GDPR imposes the strictest penalties on companies falling short on their data security commitments. India largely adopted the GDPR approach in the proposed PDPB. The Indian Committee of Experts was skeptical that its pre-PDPB laws imposed penalties stringent enough to deter undesirable conduct from IT companies.[246] Their central concern in drafting the PDPB was to promote deterrence.[247]

The California penalty approach was dramatically different from the GDPR and the PDPB. Instead of tying penalties to a corporate group's revenue, the Californian approach establishes a set monetary penalty for all companies, regardless of size.[248] Courts have narrow discretion within a limited monetary range. For claims brought by customers under their private right of action, courts also have discretion to mandate injunctive relief, which could take the form of structural reforms to the company's security infrastructure, for example. Except for the

[245] EU GDPR, Art. 34(1): "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay."
[246] *See* Committee of Experts White Paper, 191.
[247] Ibid.
[248] § 1798.150(a)(1)(A); § 1798.155(b).

injunctive relief option, the Californian law is much more predictable for companies attempting to evaluate the risks of non-compliance up-front.

The GDPR and PDPB imposed such strong penalties as a deterrence mechanism, and some initial data regarding cyber incidents parsed by GDPR compliance supports that the law has had some positive effects so far.[249] How penalties will be enforced, however, is largely still an open question. If enforcement is spotty, companies may seek to avoid detection in an attempt to eliminate the risk of the GDPR or PDPB's massive fines. Disclosure may actually decline if regulators are underfunded, under-investigate, and only enforce against select companies. The broad discretion written into those laws can create massive disparities across jurisdictions, hindering the seamless internal market that Europe in particular is trying to develop. Tying penalties to revenue is a more equitable approach, which takes into account market size and power. Lowering limits to more conservative levels, however, will still create a deterrent effect while lowering the risk of major disparities in enforcement. Lower fines will also encourage disclosure, particularly if early disclosure and cooperation with the government are rewarded in early cases.

Considering the differences between Europe and the United States regarding class actions, the choice by California to allow consumer-driven class actions is difficult to compare across jurisdictions. If regulators are unable to bear the burden of initiating enforcement actions consistently, however, considering such a plaintiff- and consumer-driven approach may be a useful alternative.

7. Summary of Recommendations

The following table summarizes the key recommendations outlined in Part 6, organized by topic area.

Topic Area	Key Recommendations
Data Breach Definition	▪ Define data breaches to include inability for authorized individuals to access their data, if the denial of access could harm them. ▪ Exempt companies from data breach notification requirements if stolen data was, and remains, properly encrypted. ▪ Require companies to periodically reassess if the encryption of stolen data remains intact. If there is a reasonable belief that the

[249] Cisco, 'Maximizing the value of your data privacy investments Data Privacy Benchmark Study,' 7.

	data has been decrypted, require companies to notify regulators and / or customers of the breach.
Security Safeguards	▪ Incorporate an obligation to periodically reevaluate security standards in light of evolving threats and the type of data being processed. ▪ Permit companies to consider cost when determining what security measures are "reasonable" or "appropriate." ▪ Continue emphasizing data encryption and pseudonymization, but require the latter to include safeguards preventing re-identification.
Regulator Notification	▪ Eliminate hour-specific notification timetables, opting for a standards-based approach. ▪ Require regulator notification only for data breaches posing a high risk to customers' rights. ▪ Begin companies' breach notification timer after they take action to mitigate immediate harms to customers from the breach, imitating the PDPB approach.
Consumer Notification	▪ Do not make customer notification contingent on regulator approval, which may create unacceptable time lags.
Penalties	▪ Tie penalties to revenue, but lower penalties to preserve deterrence while encouraging consistent reporting.

8. Conclusion

A robust international dialogue is taking place between regulators and legislators around the world engaged in the recent wave of privacy and data protection legislation. Cybersecurity strategies will be informed by these innovative new bills and laws, particularly once data measuring outcomes is collected. The choices each country and state makes in crafting its security standards will impact companies and governments around the world. Given the extraterritorial reach of many of these statutes, we can expect them to influence each other in some instances and create massive conflict of laws issues in other instances. The cybersecurity regulatory landscape today is varied, presenting an opportunity to experiment with different approaches in different contexts. Carefully assessing the approaches chosen in different jurisdictions and measuring which ones are most successful, and why, will allow us to craft stronger, less wasteful laws that can effectively balance the interests of business, the government, and consumers.

9. Bibliography

— — 2018 Data Breach Investigations Report: Executive Summary (Verizon 2018) <https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report_execsummary.pdf> accessed 24 Apr. 2019.

— — '2018 Study on Global Megatrends in Cybersecurity' *Ponemon Institute LLC* (Feb. 2018) <https://www.raytheon.com/sites/default/files/2018-02/2018_Global_Cyber_Megatrends.pdf> accessed 24 Apr. 2019.

— — 'Contract Explorer Sunburst,' *Data Lab* (Dec. 2017) <https://datalab.usaspending.gov/contract-explorer.html?search=Contract%20spending%20in%20Fiscal%20Year%202017> accessed 25 Apr. 2019.

— — 'Cyber Breaches Cause Permanent Damage to Share Values' *Fortune* (12 Apr. 2017) <http://fortune.com/2017/04/12/cyber-breaches-shareholder-damage/> accessed 24 Apr. 2019.

— — 'Cybersecurity Funding' 273 <https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_21_cyber_security-fy2019.pdf> accessed 12 May 2019.

— — 'The Equifax Data Breach' *U.S. Federal Trade Commission* <https://www.ftc.gov/equifax-data-breach> accessed 12 May 2019).

— — 'Global Cybersecurity Index (GCI) 2018,' ITU Publications (2018) <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf> ("GCI Index 2018").

— — 'Insider Threats as the Main Security Threat in 2017' *Tripwire* (11 Apr. 2017) <https://www.tripwire.com/state-of-security/security-data-protection/insider-threats-main-security-threat-2017/> accessed 24 Apr. 2019.

— — 'Learning with the Times: What is Aadhaar?' *The Times of India* (3 Oct. 2010) <https://timesofindia.indiatimes.com/india/Learning-with-the-Times-What-is-Aadhaar/articleshow/6680601.cms> accessed 25 Apr. 2019.

— — 'Ransomware Threats and Endpoint Security – An Overview' *Comodo Security Solutions* (12 Apr. 2018), https://enterprise.comodo.com/blog/ransomware-threats-and-endpoint-security-overview/> accessed 24 Apr. 2019.

— — 'Survey Shows Consumers are Abandoning Brands after Data Breaches' *Security Magazine* (23 Jan. 2019) <https://www.securitymagazine.com/articles/89777-shows-consumers-are-abandoning-brands-after-data-breaches> accessed 24 Apr. 2019.

Agarwal S, 'Justice BN Srikrishna to head Committee for data protection framework,' *The Economic Times* (New Delhi 1 Aug. 2017)

<https://economictimes.indiatimes.com/news/politics-and-nation/justice-bn-srikrishna-to-head-committee-for-data-protection-framework/articleshow/59866006.cms> accessed 25 Apr. 2019.

— — 'Personal Data Protection Bill only after new government takes over,' *The Economic Times* (New Delhi 4 Jan. 2019) <https://economictimes.indiatimes.com/tech/internet/personal-data-protection-bill-only-after-new-government-takes-over/articleshow/67374919.cms> accessed 25 Apr. 2019.

Article 29 Working Party, 'Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU' *IAPP* (11 April 2018) <https://iapp.org/media/pdf/resource_center/20180413_Article29WPStatementonencryptionePrivacypdf%20(1).pdf> accessed 16 May 2019.

Attström K et al., 'Study on the Evaluation of the European Union Agency for Network and Information Security' (*European Commission* 2016) <https://ec.europa.eu/digital-single-market/en/news/final-report-evaluation-european-union-agency-network-and-information-security-enisa> accessed 9 May 2019.

Cellerini EJ and Lang C, 'Cyber Liability: Data Breach in Europe' (July 2018), 85 Def. Couns. J. 1, 3-4.

Brody B, 'Google, Facebook Set 2018 Lobbying Records as Tech Scrutiny Intensifies' *Bloomberg* (23 January 2019) <https://www.bloomberg.com/news/articles/2019-01-22/google-set-2018-lobbying-record-as-washington-techlash-expands> accessed 10 May 2019.

Cahill K et al., 'California Consumer Privacy Act: Potential Impact and Key Takeaways' (2018) 30 No. 12 IPTLJ 11.

Byrne C, 'The new ways we could get hacked (and defended) in 2019' *Fast Company* (7 Jan. 2019) <https://www.fastcompany.com/90287253/cybersecurity-cybercrime-threats-defenses-2019> accessed 24 Apr. 2019.

CISA, 'Security Tip (ST04-015) Understanding Denial-of-Service Attacks' (*Cybersecurity and Infrastructure Security Agency (CISA)* 28 June 2018) <https://www.us-cert.gov/ncas/tips/ST04-015> accessed 24 Apr. 2019.

Cisco, 'Maximizing the value of your data privacy investments Data Privacy Benchmark Study' (January 2019) <https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/dpbs-2019.pdf> accessed 9 May 2019.

Culnane C et al., 'Health Data in an Open World,' (15 December 2017) arXiv:1712.05627 <https://arxiv.org/abs/1712.05627> accessed 16 May 2019.

Davenport A, 'CLTC Research: American Companies Struggle to Meet GDPR's Data Breach Notification Rules' *Center for Long-Term Cybersecurity* (16 May 2018)

<https://cltc.berkeley.edu/2018/05/16/cltc-research-american-companies-struggle-meet-gdprs-data-breach-notification-rules/> accessed 10 May 2019.

Division of Consumer & Business Education, 'The Marriott Data Breach' *U.S. Federal Trade Commission* (4 December 2018) <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> accessed 12 May 2019).

DLA Piper, 'DLA Piper GDPR Data Breach Survey: February 2019' (2019) 3 <https://www.dlapiper.com/en/uk/insights/publications/2019/01/gdpr-data-breach-survey/> accessed 10 May 2019.

Duggal P and Varshney R, 'India's Aadhaar Law and Cyber Security, With A Legal Eye,' Express Computer (2 May 2016) <https://www.expresscomputer.in/columns/indias-aadhaar-law-and-cyber-security-with-a-legal-eye/17347/> accessed 27 Apr. 2019.

European Commission: Cybersecurity Technology & Capacity Building (Unit H.1), 'Cybersecurity' (16 April 2016) <https://ec.europa.eu/digital-single-market/en/cyber-security> accessed 9 May 2019.

European Commission: Cybersecurity Technology & Capacity Building (Unit H.1), 'The Directive on security of network and information systems (NIS Directive)' (24 August 2018) <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive> accessed 9 May 2019.

Forbes Technology Council, 'How Will California's Consumer Privacy Law Impact The Data Privacy Landscape?' *Forbes* (20 August 2018) <https://www.forbes.com/sites/forbestechcouncil/2018/08/20/how-will-californias-consumer-privacy-law-impact-the-data-privacy-landscape/#3cb1aff3e922> accessed 10 May 2019.

Freeman DR and Koushik M, 'India Considers Stringent New Personal Data Privacy Law,' *WilmerHale* (3 Aug. 2018) <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20180803-india-considers-stringent-new-personal-data-privacy-law>.

Fruhlinger J, 'Top cybersecurity facts, figures and statistics for 2018' *CSO Online* (10 October 2018) <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html> accessed 9 May 2019.

Gelb A and Clark J, 'Performance Lessons from India's Universal Identification Program' *Center for Global Development* (May 2013) <https://www.cgdev.org/sites/default/files/biometric-performance-lessons-India.pdf> accessed 25 Apr. 2019.

Jehl L and Friel A, 'CCPA and GDPR Comparison Chart, Baker & Hostetler LLP (2018) <https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf> accessed 16 May 2019.

King J, ‘Consumers Don't Want Personalization to Get Too Personal’ *eMarketer* (26 Apr. 2018) <https://www.emarketer.com/content/consumers-don-t-want-personalization-to-get-too-personal> accessed 24 Apr. 2019.

Kirova M, ‘eIDAS Regulation (Regulation (EU) N°910/2014)’ (*European Commission* 2016) <https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014> accessed 9 May 2019.

Krishnan G, ‘Foreign agencies can access Aadhaar data’ *Sunday Guardian* (Bangalore, 25 Dec. 2011) <http://www.sunday-guardian.com/investigation/foreign-agencies-can-access-aadhar-data> accessed 25 Apr. 2019.

Lapowsky I, ‘California Unanimously Passes Historic Privacy Bill’ *Wired* (28 June 2018) <https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/> accessed 10 May 2019.

Leskin P, ‘The 21 Scariest Data Breaches of 2018’ *Business Insider* (30 Dec. 2018) <https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12> accessed 24 Apr. 2019.

Mathews K and Bowman C, ‘The California Consumer Privacy Act of 2018,’ *Proskauer* (13 July 2018) <https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/> accessed 13 May 2019.

McLaughlin M, ‘Cybersecurity and the Duty to Protect Client Data’ (2018) 91-NOV Wis. Law. 14.

McLarren C, ‘Once More Unto the Breach: How the Growing Threat of Ransomware Affects HIPAA Compliance for Covered Entities’ (2018) 15 Ind. Health L. Rev. 305.

Moody R, ‘Which countries have the worst (and best) cybersecurity?’ *Comparitech* (6 Feb. 2019), <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/.> accessed 25 Apr. 2019.

Moore S and Keen E, ‘Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019’ *Gartner* (Sydney, 15 Aug. 2018) <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019> accessed 24 Apr. 2019.

Morgan S, ‘Ransomware damage costs predicted to hit $11.5B by 2019’ *CSO* (20 Nov. 2017) <https://www.csoonline.com/article/3237674/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html> accessed 24 Apr. 2019.

Newman L, ‘The Year Cryptojacking Ate the Web’ *Wired* (24 Dec. 2018) <https://www.wired.com/story/cryptojacking-took-over-internet/> accessed 24 Apr. 2019.

O'Flaherty K, 'How to Survive a Ransomware Attack—And Not Get Hit Again' *Forbes* (17 August 2018) <https://www.forbes.com/sites/kateoflahertyuk/2018/08/17/how-to-survive-a-ransomware-attack-and-not-get-hit-again/#fa945c26cd36> accessed 23 May 2019.

Patton S, 'What is the Real Cost of a DDoS Attack?' *IoT Tech Expo* (16 Oct. 2018) <https://www.iottechexpo.com/2018/10/iot/what-is-the-real-cost-of-a-ddos-attack/> accessed 24 Apr. 2019.

Reynolds T, 'Government Contracts Insights," *Morrison & Foerster* (25 Jan. 2018) <http://govcon.mofo.com/defense/top-five-government-contractor-cybersecurity-considerations-for-2018/> accessed 25 Apr. 2019.

Rohloff K, 'Why Encryption Holds the Secret to Data Security,' *TDWI* (29 March 2019) <https://tdwi.org/articles/2019/03/29/dwt-all-why-encryption-holds-the-secret-to-data-security.aspx> accessed 16 May 2019.

Schechner S, 'Global Regulators Race to Curb Silicon Valley' *The Wall Street Journal* (10 May 2019) <https://www.wsj.com/articles/france-steps-up-global-tech-scrutiny-with-social-media-policing-11557478920?mod=hp_lead_pos4> accessed 10 May 2019.

Segarra L, 'California's Economy Is Now Bigger Than All of the U.K.' *Fortune* (5 May 2018) <http://fortune.com/2018/05/05/california-fifth-biggest-economy-passes-united-kingdom/> accessed 13 May 2019.

Skeath C and Kahn B, 'State Data Breach Notification Laws: 2018 In Review' *Covington & Burling LLP* (31 December 2018) <https://www.insideprivacy.com/data-security/data-breaches/state-data-breach-notification-laws-2018-in-review/> accessed 15 May 2019.

Stauss D et al., 'Analyzing the California Consumer Privacy Act's Private Right of Action' *Ballard Spahr LLP* (19 November 2018) <https://www.cyberadviserblog.com/2018/11/analyzing-the-california-consumer-privacy-acts-private-right-of-action/> accessed 15 May 2019.

Strategic Cyber Ventures, '2018 Cybersecurity Venture Capital Investment' (16 January 2019) <https://scvgroup.net/2018-cybersecurity-venture-capital-investment/> accessed 12 May 2019.

Tham I, 'Singapore's privacy watchdog fines IHiS $750,000 and SingHealth $250,000 for data breach,' *The Straits Times* (15 Jan. 2019) <https://www.straitstimes.com/singapore/singapores-privacy-watchdog-fines-ihis-750000-singhealth-250000-for-data-breach> accessed 25 Apr. 2019.

Tracy R and McKinnon J, 'Lawmakers Differ on Remedies for Facebook Privacy Breach' *The Wall Street Journal* (8 May 2019) <https://www.wsj.com/articles/lawmakers-differ-on-remedies-for-facebook-privacy-breach-11557343397?mod=article_inline> accessed 10 May 2019.

UIDAI, 'What Is Aadhaar?' <https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html> accessed 24 Apr. 2019.

Verizon, '2019 Data Breach Investigations Report' (May 2019) <https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf> accessed 13 May 2019.

Whittaker Z, 'California to Close Data Breach Notification Loopholes Under New Law' *Tech Crunch* (21 February 2019) <https://techcrunch.com/2019/02/21/california-data-breach-laws/> accessed 13 May 2019.

Wimmer K, 'India's Committee of Experts Releases Draft Personal Data Protection Bill,' *Covington & Burling LLP* (30 July 2019) <https://www.insideprivacy.com/international/indias-committee-of-experts-releases-draft-personal-data-protection-bill/> accessed 25 Apr. 2019.

Table of Cases

India

Table of Legislation

European Union

California

India

The Information Technology Act, 2000, No. 21 of 2000, THE GAZETTE OF INDIA EXTRAORDINARY (2000), §§ 65-67, 72, <https://www.meity.gov.in/writereaddata/files/itbill2000.pdf> accessed 27 Apr. 2019 ("IT Act, 2000")

The Information Technology (Amendment) Act, 2008, No. 10 of 2009, THE GAZETTE OF INDIA EXTRAORDINARY (2009), §§ 43A, 72A <https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf> accessed 27 Apr. 2019 ("IT Act, 2008 Amendment")

Table of Legislative Instruments

European Union

Article 29 Data Protection Working Party, 'Guidelines on Personal data breach notification under Regulation 2016/679 (3 October 2017) <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> accessed 9 May 2019 ("Personal Data Breach Guidelines").

India

Ministry of Communications and Information Technology (Department of Electronic and Information Technology) Notification, THE GAZETTE OF INDIA EXTRAORDINARY (11 Dec. 2015), <https://www.meity.gov.in/writereaddata/files/UIDAI%20CII%20notification%20Dec15.pdf> accessed 27 Apr. 2019.

See Ministry of Electronics and Information Technology Notification, The Gazette of India Extraordinary (22 May 2018), <https://www.meity.gov.in/writereaddata/files/NCIIPC-Rules-notification.pdf> accessed 27 Apr. 2019.

Ministry of Communications and Information Technology (Department of Information Technology) Notification, G.S.R. 313(E), The Gazette of India Extraordinary (2011), ¶ 8, <https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf> accessed 27 Apr. 2019 (G.S.R. 313(E) Notification).

Table of Official and Policy Documents

India

S.S. Rana & Co., 'India: Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,' *Lexology* (4 Sept. 2017), <https://www.lexology.com/library/detail.aspx?g=35f56a2a-c77c-49e7-9b10-1ce085d981dd> accessed 27 Apr. 2019.

Justice B.N. Srikrishna et al., 'White Paper of the Committee of Experts on a Data Protection Framework for India,' (2017) Ministry of Electronics and Information Technology (MeitY), 163-64 <https://innovate.mygov.in/wp-

content/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf> accessed 8 May 2019 (“Committee of Experts White Paper”).

Abstract Deutsch

Unternehmen, die für den Schutz der Kundendaten verantwortlich sind, sind einer größeren Anzahl und Vielfalt von Cyber-Bedrohungen ausgesetzt. Infolgedessen hat in vielen Ländern der öffentliche Druck zugunsten strengerer Datenschutzanforderungen zugenommen, was zum Vorschlag oder zur Verabschiedung von einschlägigen Rechtsvorschriften geführt hat. In dieser Arbeit werden die geforderten Sicherheitsanforderungen in drei Datenschutzgesetzen in der Europäischen Union, den USA und Indien analysiert: der Datenschutz-Grundverordnung (DSGVO), dem kalifornischen Verbraucherschutzgesetz (CCPA) bzw. dem Gesetz zum Schutz personenbezogener Daten (PDPB). Die Arbeit vergleicht ihre Ansätze zur Definition eines Verstoßes, umreißt das Sicherheitsniveau, das zur Vermeidung von Haftung erforderlich ist, und setzt sich mit den geforderten Meldungen von Aufsichtsbehörden und Verbrauchern und den allenfalls zu verhängenden Sanktionen auseinander. Auf der Grundlage dieser Analyse werden allgemeine Grundsätze für die künftige Gesetzgebung empfohlen.

In Zusammenhang mit der Definition von Datenschutzverletzungen wird insbesondere Indien und die umfassendere Definition durch die EU beleuchtet, die den Verlust des Zugriffs auf Daten einschließt. In dieser Arbeit wird empfohlen, dass die USA Zugriffsverweigerungen ausdrücklich in ihre Datenschutzgesetze aufnehmen, anstatt sich auf Ad-hoc-Interpretationsrichtlinien zu stützen. Alle drei Rechtsordnungen stützen sich auf einen „Angemessenheits-“ oder „Vernünftigkeits-“ Standard für Sicherheitsmaßnahmen. Sie variieren in Bezug auf spezifische Anforderungen, z. B. hinsichtlich der Möglichkeit eines Unternehmens, Kosten bei der Bewertung seiner Sicherheitspflichten zu berücksichtigen. In dieser Arbeit wird empfohlen, Kostenüberlegungen zuzulassen und Vorgaben festzulegen, dass Sicherheitsstandards regelmäßig überprüft werden, sofern diese fehlen. In Indien und den USA basieren die Notifizierungszeitpläne auf Standards, in der DSGVO hat die EU jedoch einen strengen 72-Stunden-Zeitplan festgelegt. In dieser Arbeit wird empfohlen, die Notifizierungszeitpläne der DSGVO zu streichen und den Umfang der zu meldenden Verstöße zu begrenzen, um das Risiko eines Rückstands bei den Aufsichtsbehörden zu verringern. Schließlich wird in dieser Arbeit empfohlen, die Strafen auf der Grundlage der Einnahmen des Unternehmens zu berechnen und die entsprechenden DSGVO- und PDPB-Werte zu senken.

Abstract English

Companies tasked with safeguarding consumers' data are facing a greater number and variety of cyber threats. Consequently, many countries have experienced a surge in public pressure in favor of more stringent data protection requirements, resulting in the proposal or passage of legislation. This paper analyzes the security requirements in three pieces of data protection legislation in the European Union, the United States, and India—the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Personal Data Protection Bill (PDPB), respectively. It compares their approaches to defining a breach, outlining the level of security needed to avoid liability, requiring regulator and consumer notifications, and imposing penalties. Based on this analysis, it recommends general principles to include in future legislation.

The breach definition highlights India and the EU's broader definition of a data breach, which includes loss of access to data. This piece recommends that the United States explicitly incorporate access denials into its data protection laws, rather than relying on ad hoc interpretive guidelines. All three jurisdictions rely on an "appropriateness" or "reasonability" standard for security safeguards. They vary in more specific requirements, such as the ability of a company to consider cost when evaluating its security obligations. This paper recommends permitting cost considerations and adopting requirements to periodically reevaluate security standards, where they are absent. Notification timetables are standards-based in India and the United States, but the EU adopted a strict 72-hour timetable in the GDPR. This paper recommends eliminating GDPR-style timetables and limiting the scope of breaches requiring notification to mitigate the risk of regulator backlog. Finally, this paper recommends calculating penalties based on company revenue, but lowering them from the GDPR and PDPB levels.