What Is a "Reasonable Security Procedure and Practice" Under the California Consumer Privacy Act's Safe Harbor?

Scott J. Hyman, Genevieve R. Walser-Jolly, and Elizabeth Farrell

Scott J. Hyman

Genevieve R. Walser-Jolly

Elizabeth Farrell

Scott J. Hyman is a shareholder with Severson & Werson, and holds both European and U.S. Certified Information Privacy Professional credentials with the International Association of Privacy Professionals. Mr. Hyman is a Certified Information Privacy Manager and is the Firm's Data Protection Officer. Mr. Hyman is a Vice President of the Conference on Consumer Finance Law.

Genevieve R. Walser-Jolly is a member of Severson & Werson, is the Member-in-Charge of the Firm's Orange County Office, and holds a U.S. Certifed Information Privacy Professional credential with the International Association of Privacy Professionals. Ms. Walser-Jolly is the author of the California Continuing Education of the Bar's Treatise on the California Consumer Privacy Act.

Elizabeth Farrell is a litigation associate in Severson & Werson's Orange County office and a member of the Financial Services Litigation Practice Group. Ms. Farrell received her J.D. from the University of San Diego, where she served on the Editorial Board of the San Diego Law Review.

I. Introduction 174
II. The California Consumer Privacy Act 178
A. Summary of the CCPA 178
1. *Disclosure requirements* 178
2. *Responding to verifiable consumer requests* 179
3. *Exemptions from the CCPA* 179

4. *Remedies under the CCPA* 180
III. "Reasonable Security Procedures and Practices" Under the CCPA 181
A. Legislative and Regulatory Background 181
B. "Reasonable" Means What It Says 193
1. *The CCPA's common law roots* 193
a. Foreseeability and risk/utility 193
b. Cybersecurity does not justify varying from the reasonableness principles that the CCPA incorporates 197
2. *Statutory analogies: "reasonable policies and procedures" defenses* 202
IV. Conclusion 207

I. Introduction

Effective January 1, 2020, the California Consumer Protection Act (CCPA) will provide California consumers with a private right of action if their unencrypted and unredacted personal information is the subject of a data breach that results from a business's failure to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information[.]"[1] Victimized consumers may recover damages between $100 and $750 per consumer per incident, or actual damages, whichever is greater.[2] Potential liability turns on the seriousness of the violations, the number of violations, the length of time over which violations occurred, the willfulness of the business's conduct, and the business's assets, liabilities, and net worth.[3] Accordingly, because the California Legislature passed the CCPA in 2018, businesses have rushed to implement or shore up their privacy practices and cybersecurity procedures before the CCPA's January 1, 2020 effective date to avoid potentially catastrophic class-wide liability for a data breach.

But what constitutes a "reasonable security procedure and practice" under the CCPA's "safe harbor"?[4] The CCPA provides little guidance, merely

1. Cal. Civ. Code § 1798.150(a)(1).
2. *Id*. § 1798.150(a)(1)(A). Consumers may also recover injunctive relief or any other relief that the court deems proper. *Id*. § 1798.150(a)(1)(B)–(C).
3. *Id*. § 1798.150(a)(2).
4. We use the term "defense" and "safe harbor" for literary license only. The term safe harbor suggests an affirmative defense on which the defendant bears the burden of proof, and some commentators have suggested, without authority, that "reasonable procedures" under the CCPA is a defense or safe harbor. Brandon H. Graves & Svetlana McManus, *"Reasonable Security"—The Myth of the CCPA Safe Harbor*, DWT: Privacy & Security Law Blog (May 9, 2019), https://www.dwt.com / blogs / privacy--security-law-blog / 2019 / 05 / reasonable-security-the-myth-of-the-ccpa-safe [https://perma.cc/B9GC-EP4X] ("The CCPA by its terms provides a defense for companies that employ 'reasonable security.'"). Nothing in the CCPA, however, suggests that a business's failure

tying the reasonableness of the security procedure and practice to the nature of the information. The CCPA's "appropriate to the nature of the information" clause suggests that the specialty of the data itself can affect the type and extent of the security procedures and practices a business must implement.

The CCPA was supposed to receive interpretive regulations from the California Attorney General regarding the reasonable procedure and practice clause and other provisions before the January 1, 2020 effective date. The Attorney General issued proposed regulations on October 11, 2019—none of which, however, relate to what constitutes a reasonable security procedure and practice under the CCPA.[5] True, the Attorney General previously provided a Data Breach Report in 2016 that preceded CCPA's enactment.[6] But the Attorney General's Report, by its own terms, is neither binding nor entitled to deference,[7] and, arguably, improperly advocates a

to maintain reasonable security procedures and practices under the CCPA is an affirmative defense rather than an element of the plaintiff's cause of action on which the plaintiff bears the burden of proof. *See*, *e.g.*, Anderson v. Kimpton Hotel & Rest. Grp., LLC, Case No. 19-cv-01860-MMC, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019) ("As Kimpton points out, however, plaintiffs fail to allege any facts in support of their conclusory assertion that Kimpton violated § 1798.81.5 by 'failing to implement and maintain reasonable security procedures and practices.'"); *see also infra* notes 52–58.

5. No. 41-Z Cal. Regulatory Notice Reg. 1341–50 (Oct. 2019) (to be codified at Cal. Code Regs., tit. 11 §§ 999.300–999.341).

6. Kamala D. Harris, Attorney General, Cal. Data Breach Report 2012–2015 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf [https://perma.cc/2YL9-733A] [hereinafter 2016 Breach Report].

7. The Attorney General's Data Breach Report is neither a regulation nor an "opinion" requested by an officer or agency. By its terms, the Report does not reflect the Attorney General's enforcement position. *Id.* ("This document is for informational purposes and should not be construed as legal advice or as policy of the State of California."). Even if the Report could be interpreted to rise to the level of an opinion, which it is not, it would not be binding. *Legal Opinions of the Attorney General—Frequently Asked Questions*, Cal. Office of the Att'y Gen., https://oag.ca.gov/opinions/faqs [https://perma.cc/33FJ-ETKP] ("The Attorney General's opinions are advisory, and not legally binding on courts, agencies, or individuals. Nonetheless, Attorney General's opinions are usually treated as authoritative by the officers and agencies who have requested them. In addition, Attorney General's opinions are often treated as persuasive authority by courts. Courts have expressed this idea in several ways, including: 'Although an official interpretation of a statute by the Attorney General is not controlling, it is entitled to great respect.' 'Opinions of the Attorney General, while not binding, are entitled to great weight. In the absence of controlling authority, these opinions are persuasive "since the legislature is presumed to be cognizant of that construction of the statute."'" (citations omitted) (first quoting Thorning v. Hollister Sch. Dist., 15 Cal. Rptr. 2d 91, 94 (Cal. Ct. App. 1992);

one-size-fits-all standard that is both more stringent than the CCPA's reasonable procedures and practices and, conceptually, has been rejected by consumer commentators and other privacy legislation.

Like the Attorney General's Data Breach Report, many in the data privacy industry seem to have bypassed traditional rules of "reasonableness" and advocated for a technical, one-size-fits-all security-based standard,[8] or

then quoting Napa Valley Educators' Ass'n v. Napa Valley Unified Sch. Dist., 239 Cal. Rptr. 395, 399 (Cal. Ct. App. 1987))).

8. *See* Stan, *CCPA and Minimum Reasonable Security Procedures and Practices: A Floor on "Defendability,"* Citadel Info. Group (June 12, 2019), https://citadel-information.com/2019/06/minimum-reasonable-security-procedures-and-practices-a-floor-on-defendability/ [https://perma.cc/7N9U-U95E] ("The NIST Cybersecurity Framework is a logical contender for what constitutes *reasonable security.* The Framework though does not include—nor is it intended to include—*security procedures and practices.* It is intended, instead, as the basis upon which an organization can develop its *reasonable security procedures and practices.* In the California 2016 Data Breach Report, then Attorney General Kamala Harris wrote *'The 20 controls in the Center for Internet Security's Critical Security Controls [CIS-20] define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.'*") (emphasis in original). The International Organization for Standardization (ISO) Standards now include both technical and management protocols. *ISO Publishes First International Standards for Privacy Information Management*, IAPP: Daily Dashboard (Aug. 7, 2019), https://iapp.org/news/a/iso-publishes-first-international-standards-for-privacy-information-management/ [https://perma.cc/52RA-9N26] ("The International Organization for Standardization has published the first International Standards for privacy information management. ISO/IEC 27701 specifies requirements 'for establishing, implementing, maintaining and continually improving a privacy-specific information security management system,' ISO said in the announcement."); *see also Frequently Asked Questions*, NIST: Privacy Framework, https://www.nist.gov/privacy-framework/frequently-asked-questions [https://perma.cc/F9JM-MRDF] (discussing the National Institute of Standards and Technology's (NIST) development of "a voluntary privacy framework, in collaboration with private and public sector stakeholders" intended to better identify, assess, manage, and communicate privacy risks; foster the development of innovative approaches to protecting individuals' privacy; and increase trust in products and services). Reliance on NIST or other private party standards, therefore, is not dispositive. Moreover, businesses should take caution before developing security procedures and practices based on NIST, as even the Federal Trade Commission staff has found fault with NIST standards. *See* Fed. Trade Comm'n, Staff Comment on the Preliminary Draft for the NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management pt. III, at 8 (Oct. 24, 2019), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-preliminary-draft-nist-privacy-framework/p205400nistprivacyframeworkcomment.pdf [https://perma.cc/93V6-JZTD] [hereinafter FTC Comment on NIST] (recommending and enumerating five suggestions for the NIST to consider for its forthcoming proposed privacy framework).

a "reasonable cyber-security professional" standard.[9] Trial lawyers who litigate CCPA data breach claims and judges who preside over such claims will, however, have to interpret the CCPA's reasonable procedures and practices standard and whether the CCPA requires a higher standard of reasonableness than the law traditionally has recognized simply because consumer data is involved or because cybersecurity is technical in nature.

This article explores the CCPA's reasonable procedures and practices standard. The article draws from the CCPA's legislative history and the well-established negligence principles on which the CCPA's term "reasonable" is based. This article proposes that a reasonable procedures and practices standard means what it says, and does not require perfection,[10] state-of-the-art cybersecurity,[11] or a financial commitment that bankrupts a company or stifles innovation. Rather, reasonableness evaluates all of the particular circumstances and balances the burden of precaution against the nature of the data held, the foreseeability of injury to the data subjects in light of the nature of the data held, and the business's degree of control over the risk.

9. Abraham Kang, *What is "Reasonable Security"? And How to Meet the Requirement*, CSO (Apr. 23, 2019, 3:00 AM), https://www.csoonline.com/article/3390150/what-is-reasonable-security-and-how-to-meet-the-requirement.html [https://perma.cc/YYG3-H8QJ] ("Another important distinction is that there are professional standards of care. . . . Security professionals are no different than other professionals because they market their specialized skills (risk assessments, security design review, forensic examinations, pen testing, malware analysis, security code review analysis, etc.) to protect and secure the company's enterprise systems. Therefore, it is likely for security professionals to fall under the professional standard of care. Professional standards of care are more strict than the ordinary prudent person standard and have the potential to increase liability.").

10. "[T]here cannot be 'perfect' security and . . . data breaches can occur even when a company takes reasonable precautions to prevent them." *In re* Twitter, Inc., Docket No. C-4316, 2011 WL 914034, at *17 (F.T.C. Mar. 2, 2011). "[T]he fact of a breach does not mean that a company has failed to honor a promise to maintain reasonable security." *Id.* at *19.

11. Razuki v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 2761818, at *2 (S.D. Cal. June 8, 2018) ("[Razuki has] alleged Caliber intentionally violated his privacy by choosing to implement low-budget security measures with an 'absolute disregard of its consequnces.' . . . The Court acknowledges that Razuki probably cannot make specific and definitive allegations about how Caliber's Security was insufficient before discovery. But he needs to hum a few more bars about some of those allegations . . . ."). On Razuki's fourth amended complaint, the court dismissed the cause with prejudice for failing to state specific facts to support the allegation that Caliber's security measures were insufficient. Razuki v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 6018361, at *3 (S.D. Cal. Nov. 15, 2018).

II. The California Consumer Privacy Act

A. Summary of the CCPA.

The CCPA shifts the conversation about who owns, or controls, the personal information[12] of California residents collected by businesses.[13] In this vein, the CCPA empowers California residents (i.e., "consumers" under the CCPA)[14] with six new rights:

1. The right to know what personal information is collected about them;
2. The right to know if their personal information is shared or sold and to whom;
3. The right to prohibit the sale of their personal information;
4. The right to access their personal information;
5. The right to have their personal information deleted; and
6. The right to not be discriminated against for exercising their rights under the CCPA.

1. Disclosure requirements.

Before a business can collect personal information, it must disclose what categories of data will be collected, the source of the personal information, who the information is shared with, and the purpose of sharing.[15] Businesses must also advise consumers of their right to request disclosure of categories and specific pieces of personal information collected about them;[16] the right to know what data is sold or shared;[17] the right to be

12. "'Personal information' means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code § 1798.140(o)(1) (West 2020).

13. A "business" is a "sole proprietorship, partnership, limited liability company, corporation, association," or other for profit legal entity "that collects consumers' personal information," or has such information is collected on its behalf. *Id.* § 1798.140(c)(1)(A). A business is covered under the CCPA if it has (1) annual gross revenue in excess of $25,000,000; (2) "annually buys, receives for commercial purposes, sells, or shares for commercial purposes, . . . the personal information of 50,000 or more consumers, households, or devices"; or (3) "derives 50 percent or more of its annual revenue from selling personal information." *Id.* § 1798.140(c)(1)(A)–(C). The term "business" includes any "entity that controls or is controlled by a business." *Id.* § 1798.140(c)(2).

14. *Id.* § 1798.140(g).

15. *Id.* § 1798.100(b).

16. *Id.* § 1798.100(a).

17. *Id.* §§ 1798.115(a)(2)–(3).

forgotten (i.e., to request deletion of collected data);[18] and the right to not be discriminated against for exercising their rights.[19]

If a business sells consumer personal information to third parties, then it must also advise consumers of their right to opt-out, and the business must include a link to that effect on the "Do Not Sell My Personal Information" page.[20]

2. Responding to verifiable consumer requests.

A business must respond to verifiable consumer requests.[21] The business's response will depend on the type of request. For example, if a consumer requests disclosure of the personal information collected, the business must provide the consumer with a list of categories and/or specific pieces of personal information collected.[22]

A business that sells personal information, or discloses personal information for a business purpose, must disclose to the consumer: (1) categories of personal information collected; (2) categories of personal information sold; (3) categories of third parties to whom personal information is sold (by category of personal information sold); and (4) categories of personal information disclosed for a business purpose.[23] If the business has not sold or disclosed personal information of consumers for a business purpose, the business must let the consumer know that fact.[24]

If a consumer makes a verifiable request for deletion, the business and its service providers must comply, unless an exception applies.[25]

3. Exemptions from the CCPA.

Depending on how it was obtained and its purpose, personal information may be exempt from the CCPA. For example, personal information that is collected and used pursuant to the Health Insurance Portability and Accountability Act of 1996 or the Health Information Technology for Economic and Clinical Health Act is exempt.[26] The CCPA also exempts medical information collected by a qualifying health care provider under the California Confidentiality of Medical Information Act.[27]

---

18. *Id.* § 1798.105(a).
19. *Id.* § 1798.125(a).
20. *Id.* §§ 1798.120(a), 1798.135(a)(1).
21. A "verifiable consumer request" for purposes of the CCPA means a request by (1) a consumer; (2) a consumer on behalf of his or her minor child; or (3) "a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify . . . ." *Id.* § 1798.140(y).
22. *Id.* § 1798.100(c).
23. *Id.* §§ 1798.115(a)(1)–(3).
24. *Id.* § 1798.115(c)(2).
25. *Id.* §§ 1798.105(c)–(d).
26. *Id.* § 1798.145(c)(1)(A).
27. *Id.*

The CCPA does not apply to personal information collected, maintained, disclosed, sold, communicated, or used when bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher under the Fair Credit Reporting Act.[28]

Data that a business or financial institution collects, processes, sells, or discloses "pursuant" to the Gramm-Leach-Bliley Act or the California Financial Information Privacy Act is exempt from the CCPA.[29] Lastly, the CCPA does not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994.[30]

4. Remedies under the CCPA.

The CCPA confers on consumers a private right of action if their unencrypted and unredacted personal information[31] is the subject of a data breach that results from a business's failure to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information[.]"[32] Consumers may recover damages between $100 and $750 per consumer per incident or actual damages, whichever is greater.[33] Consumers may also obtain injunctive relief or any other relief that the court deems proper.[34] In determining the amount of damages, courts may consider the relevant circumstances, the seriousness of the violations, the number of violations, the length of time over which violations occurred, the willfulness of the business's conduct, and the business's assets, liabilities, and net worth.[35]

28. *Id*. § 1798.145(d).
29. *Id*. § 1798.145(e).
30. *Id*. § 1798.145(f).
31. For purposes of remedies, lost personal information that can give rise to a cause of action is narrower than the CCPA's definition of "personal information." Personal information that can give rise to a private right of action under the Act is limited to unique biometric data, government issued identification numbers (e.g., social security number; passport number; tax identification number; military identification number; driver's license number or California identification card number); an "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"; medical information; and health insurance information. *Id*. § 1798.81.5(d)(1)(A)(i)–(vi), *as amended by* Act of Oct. 11, 2019, ch. 750, §2, 2019 Cal. Legis. Serv. 750 (West). In recent years, the concept of identifiable data has steadily developed in the United States. Daniel J. Solove & Paul M. Schwartz, *ALI Data Privacy: Overview and Black Letter Text* 12–14 (Geo. Wash. Law Sch. Pub. L. & Legal Theory Paper No. 2019-67), available at http://dx.doi.org/10.2139/ssrn.3457563 [https://perma.cc/BY8B-K7QL].
32. Civ. § 1798.150(a).
33. *Id*. § 1798.150(a)(1)(A).
34. *Id*. §§ 1798.150(a)(1)(B)–(C).
35. *Id*. § 1798.150(a)(2).

Before filing suit for statutory damages, a consumer must notify the business of the alleged wrongdoing and provide the business 30 days to cure.[36] If a cure is possible and completed, the business must provide the consumer with written notice of the cure and a statement that no further violations will occur.[37] While it is unclear from a practical perspective how a business could "cure" a data breach, the law in other contexts recognizes a business's ability to do so.[38] Nonetheless, if these requirements are met, the consumer may not file a lawsuit (individually or on a class-wide basis) for statutory damages, unless and until future violations occur.[39] No notice is required prior to filing an action for actual pecuniary damages.[40]

III. "Reasonable Security Procedures and Practices" Under the CCPA

A. Legislative and Regulatory Background.

Although passed in record time,[41] the California Legislature did not enact the CCPA in a vacuum. Data privacy is far from a new concept in

36. *See* Genevieve Walser-Jolly & Scott Hyman, *The California Consumer Privacy Act's 30-Day Right to Cure* (ABA Sec. Bus. Law/Consumer Fin. Servs. Committee Newsl.), Nov. 2019.

37. Civ. § 1798.150(b).

38. *See* Timlick v. NCB Mgmt. Servs., No. A152467, 2019 WL 3298779, at *1 (Cal. Ct. App. July 23, 2019) (applying the Rosenthal Act's 15-day cure provision to a type-size violation); Timlick v. Nat'l Enter. Sys., Inc., 247 Cal. Rptr. 3d 575, 583–85 (Cal. Ct. App. 2019) (holding there were defenses available under the Rosenthal Act for cured violations); Romero v. Department Stores Nat'l Bank, 725 Fed. App'x 537, 539 (9th Cir. 2018) ("[T]he defense does not apply if the creditor cannot undo the harm to a debtor that its violation has already caused."); Watkins v. Inv. Retrievers, Inc., No. 2:17-cv-01348-KJM-CKD, 2018 WL 558833, at *5–6 (E.D. Cal. Jan. 24, 2018) (stating Watkins may be able to cure his deficiencies). *See also supra* note 37.

39. Civ. § 1798.150(b).

40. *Id*.

41. Cynthia J. Cole, *California in the Data Privacy Spotlight: California Passes Sweeping Data Privacy Law in Record Time*, Baker Botts: Insights (July 5, 2018), http://www.bakerbotts.com/insights/publications/2018/07/california-in-the-data-privacy-spotlight [https://perma.cc/W5RY-8H4G] ("California was already leading the charge on individual state privacy legislation in the US when on June 28, 2018, just one week after its proposition, the California Consumer Protection Act . . . was passed and signed into law as AB 375 . . . . The rapid turnaround for this bill is due to a ballot initiative of the same name that, after having reached double the required number of signatures, was set for a vote in November 2018. This ballot initiative sought to bring many of the protections of the GDPR to the U.S. and was in many ways a much stronger predecessor to the Act. The threat of the initiative going onto the November ballot—and having a very favorable 80% positive advance polling—spurred California legislators into action on the bill. The Act being very much a compromise from

California. For example, California's Constitution guarantees the right to privacy,[42] and that right has long been protected through the state's adoption of consumer privacy laws. And, before the CCPA was enacted, privacy laws like the Information Practices Act of 1977 limited the collection of personal information by state agencies.[43]

Passed recently, the California Consumer Records Act (CRA)[44] requires certain businesses to safeguard Californians' personal information. Specifically, the CRA requires businesses to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information [.]"[45]

If the CRA's language sounds familiar, it should. The CCPA draws from the CRA's statutory language, although the CCPA expands the CRA's damages scheme for security breaches.[46] Given the statutes' identical language, it makes sense to examine the CRA for guidance in determining what constitutes a "reasonable" security policy and procedure under the CCPA.[47]

---

the ballot initiative. State technology and business lobbies were vehemently opposed to the ballot initiative, and they saw the CCPA bill as the lesser of two evils. Per the compromise between legislators and the initiative's proponents, the initiative was withdrawn after the June 28, 2018 passage of the CCPA bill—literally hours before the deadline to withdraw November 2018 ballot initiatives.").

42. Cal. Const. art. I, § 1.

43. Civ. §§ 1798–1998.77.

44. Notably, in 2004, California became one of the

> [F]irst states to enact legislation that imposes security duties on all organizations that maintain personal information. The two houses of its legislature passed two pieces of legislation, Senate Bill ("S.B.") 1386, and Assembly Bill ("A.B.") 1950. These laws create a series of affirmative duties to secure personal data for all companies that maintain the personal information of one or more California residents. These duties include notifying individuals when their information is released, either purposefully or inadvertently. It also requires companies to "provide reasonable security" for personal information, including developing and implementing "reasonable security measures" for protecting the information. It further requires that an organization's subcontractors also implement such measures.

Derek A. Bishop, *To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information*, 3 Shidler J. L. Com. & Tech. 1, ¶ 11 (2006).

45. Civ. § 1798.81.5(b).

46. Under section 1798.81.5 of the California Civil Code, consumers were required to prove actual damages. *E.g.*, Hameed-Bolden v. Forever 21 Retail, Inc., Case No. CV 18-03019 SJO (JPRx), 2018 WL 6802818, at *7 (C.D. Cal. Oct. 1, 2018).

47. Civ. § 5 ("The provisions of this Code, so far as they are substantially the same as existing statutes or the common law, must be construed as continuations thereof, and not as new enactments.").

The CRA's legislative history supports applying the tort law standard of reasonableness, stating that it "rel[ies] on the 'reasonableness' standard already well-established by tort law."[48] The case law discussing pleading requirements under the CRA, however, often focuses on the technical aspects of a business's security procedures rather than the reasonableness of the procedures.

In *In re Adobe Systems Privacy Litigation*,[49] for example, the district court described Adobe's security practices and procedures in concluding that Plaintiffs had Article III standing. The district court described the Plaintiffs' allegations that Adobe had failed to maintain reasonable security procedures as follows: (1) "researchers concluded that Adobe's security practices were deeply flawed and did not conform to industry standards"; (2) although customers' passwords had been stored in encrypted form, independent security researchers analyzing the stolen passwords discovered that Adobe's encryption scheme was poorly implemented, such that the researchers were able to decrypt a substantial portion of the stolen passwords in short order; and (3) Adobe failed to employ intrusion detection systems, properly segment its network, or implement user or network level system controls.[50]

By contrast, in *Razuki v. Caliber Home Loans, Inc.*,[51] the district court found deficient the mere allegation that the "[d]efendant knew of higher-quality

48. *Privacy: Personal Information, Hearing on A.B. 1950 Before the S. Comm. on the Judiciary*, 2003–2004 Leg., Reg. Sess. 4 (Cal. 2004) [hereinafter *Hearing on A.B. 1950*] ("[T]he goal of the bill is to provide a minimum standard of protection to personal information not covered by existing privacy laws. The bill would not set forth a specific standard, but instead rely on the 'reasonableness' standard already well-established by tort law.").

49. *In re* Adobe Sys., Inc., 66 F. Supp. 3d 1197, 1206–07 (N.D. Cal. 2014).

50. Similarly, other courts have held that a data breach combined with failure to encrypt data was a sufficient allegation of failure to maintain reasonable security measures sufficient to survive a motion to dismiss. *See* Dugas v. Starwood Hotels & Resorts Worldwide, Inc., Case No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *10 (S.D. Cal. Nov. 3, 2016) ("While it is true that Plaintiff's FACC is short on specifics, one allegation that does gives some indication of how Defendants' cybersecurity was supposedly insufficient states that 'Starwood, among other things, failed to "appropriately encrypt customers" data in its possession.' Plaintiff separately suggests that Defendants' 'security systems and protocols' should have been designed, implemented, maintained, and tested 'consistent with industry standards and requirements.'") (citation omitted); *see also In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (pleading failure to maintain reasonable security measures by alleging that Plaintiffs gave personal information to Sony as part of commercial transaction, and that Sony failed to employ reasonable security measures to protect the information, including failing to use industry-standard encryption).

51. Razuki v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 6018361 (S.D. Cal. Nov. 15, 2018).

security protocols available to them but failed to implement these measures."[52] The district court explained:

> Razuki makes a conclusory statement that Caliber knew of higher-quality security measures, but he does not support that conclusion with any facts about Caliber's protocols or actions it took when choosing appropriate security measures. All section 1798.81.5 requires is that a business "implement and maintain reasonable security procedures and practices appropriate to the nature of the information." Razuki could have identified what made Caliber's security measures unreasonable by comparison to what other companies are doing, but simply knowing of higher-quality security measures is not sufficient to state a claim. Further, Razuki's TAC says that "Caliber's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the personal and financial information of Plaintiff and the other Class members." The Court has already acknowledged that it may be difficult to definitively show Caliber's practices were insufficient prior to discovery, but again, he needs something more than what he's pleading now. What facts lead him to believe Caliber didn't comply with industry standards? What are other companies doing that Caliber isn't? These are basic questions that Razuki could plead to plausibly show Caliber's conduct was unlawful. Instead, it appears he's simply recited a few buzz words with the hope that he may be able to figure out later what, if anything, Caliber has done wrong.[53]

In *Anderson v. Kimpton Hotel & Restaurant Group, LLC*,[54] Judge Chesney dismissed a data breach claim under section 1798.81.5 of the Civil Code because the plaintiffs plead no facts, other than the data breach itself, to support their contention that the defendant failed to maintain reasonable security measures.[55] The developing case law indicates courts will not hesitate to dispose of cases where a data-breach plaintiff fails to establish a duty of care.[56]

---

52. *Id*. at *1. *But see Hameed-Bolden*, 2018 WL 6802818, at *4 ("Plaintiffs meet the broad standards set out in the UCL. In the FAC, Plaintiffs alleged that Defendants engaged in unlawful and unfair practices within the meaning of the UCL because Defendants failed to employ reasonable, industry standard, and appropriate security measures, misrepresented the safety of its many systems and services, the security thereof, their ability to store Customer Data, and violated section 5 of the Federal Trade Commission Act. This is enough to survive the instant Motion.") (citation omitted).

53. *Razuki*, 2018 WL 6018361, at *1–2 (citations omitted).

54. Anderson v. Kimpton Hotel & Rest. Grp., LLC, Case No. 19-cv-01860-MMC, 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019).

55. *Id*. at *7–9; *see also* Smith v. Sabre Corp., No. 2:17-cv-05149-SVW-AFM, 2017 U.S. Dist. LEXIS 221783, at *14 n.1 (C.D. Cal. Oct. 23, 2017) ("Plaintiffs fail to allege how Sabre failed to employ "reasonable security procedures" as required for a violation of Cal. Civ. Code § 1798.81.5. Plaintiffs plead no facts at all regarding Sabre's data security practices. Instead, they suggest that any time a company is the victim of theft by a third party criminal, security deficiencies should be implied. The law is to the contrary: "Nile's implied premise that be-

From a pleading and evidentiary standpoint, at least, the CRA's reasonableness requirement thus requires something more than the data breach itself, or the existence of better security measures.[57] However, the decisions interpreting the CRA provide little guidance on what a reasonable security measure "is"—suggesting, instead, what "is not" (i.e., what is *un*reasonable). Regulatory agencies also seem to follow this same approach. The FTC, for example, also defines reasonable security measures by defining such measures in the negative—i.e., focusing on what constitutes *un*reasonable security measures.[58] It is true that the FTC has given guidance on

---

cause data was hacked[,]" the "protections must have been inadequate is a 'naked assertion[] devoid of further factual enhancement' that cannot survive a motion to dismiss." (quoting Kuhns v. Scottrade, Inc., 868 F.3d 711, 717 (8th Cir. 2017))).

56. Silverpop Sys. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 852 (11th Cir. 2016) ("Here, assuming, *arguendo*, that Silverpop had a duty to conform its conduct to a particular standard to protect against incidents resulting in a data breach, LMT has failed to present evidence to establish the applicable standard of care. "Evidence of custom within a particular industry, group, or organization is admissible as bearing on the standard of care in determining negligence." Silverpop contends that LMT's expert has not proposed any standards that are ordinarily employed in Silverpop's industry, and LMT fails to rebut this contention. Overall, while LMT highlights several deficiencies in Silverpop's intrusion detection system, it offers no evidence to establish how Silverpop's practices, as they related to intrusion detection, failed to meet the applicable standard of care. Accordingly, as LMT has failed to present evidence establishing the standard of care that governed Silverpop's actions, it cannot establish a breach of the standard of care.") (citations omitted).

57. *C.f.* Hapka v. CareCentrix, Inc., Case No. 16-2372-CM, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016) ("Plaintiff responds that defendant's duty is to exercise reasonable care when it collects and stores the personal information of its employees. In this instance, defendant was obligated to implement reasonable data security measures to protect that information from disclosure. The court agrees with plaintiff that requiring identification of a statutory duty is unnecessary. Given plaintiff's allegations that the harm was foreseeable, defendant had the duty to exercise reasonable care to prevent that harm. The court will not dismiss plaintiff's claim for failure to identify a more specific duty.") (citation omitted).

58. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 252, 255 (3d Cir. 2015) ("Wyndham argues it was entitled to 'ascertainable certainty' of the FTC's interpretation of what specific cybersecurity practices are required by § 45(a). Yet it has contended repeatedly—no less than seven separate occasions in *this* case—that there is no FTC rule or adjudication about cybersecurity that merits deference here. The necessary implication, one that Wyndham itself has explicitly drawn on two occasions noted below, is that federal courts are to interpret § 45(a) in the first instance to decide whether Wyndham's conduct was unfair. . . . We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC's interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether

a "fundamental" security threshold, a cybersecurity floor that involves ten basic precepts:

> (1) Start with security; (2) Control access to data sensibly; (3) Require secure passwords and authentication; (4) Store sensitive personal information securely and protect it during transmission; (5) Segment your network and monitor who's trying to get in and out; (6) Secure remote access to your network; (7) Apply sound security practices when developing new products; (8) Make sure your service providers implement reasonable security measures; (9) Put procedures in place to keep your security current and address vulnerabilities that may arise; [and] (10) Secure paper, physical media, and devices.[59]

Wyndham had fair notice that its conduct could fall within the meaning of the statute."); LabMD, Inc. v. FTC, 894 F.3d 1221, 1236 (11th Cir. 2018) ("In the case at hand, the cease and desist order contains no prohibitions. It does not instruct LabMD to stop committing a specific act or practice. Rather, it commands LabMD to overhaul and replace its data-security program to meet an indeterminable standard of reasonableness. This command is unenforceable. Its unenforceability is made clear if we imagine what would take place if the Commission sought the order's enforcement. As we have explained, the standards a district court would apply are essentially the same whether it is entertaining the Commission's action for the imposition of a penalty or the Commission's motion for an order requiring the enjoined defendant to show cause why it should not be adjudicated in contempt. For ease of discussion, we posit a scenario in which the Commission obtained the coercive order it entered in this case from a district court, and now seeks to enforce the order."); *see also* Graves & McManus, *supra* note 4 ("The FTC has been happy to point out what it believes '*un*reasonable security' is but less eager to specify what constitutes 'reasonable security.'"); Patricia Bailin, *Study: What FTC Enforcement Actions Teach Us About the Features of Reasonable Privacy and Data Security Practices*, IAPP (Sept. 19, 2014), https://iapp.org/media/pdf/resource_center/FTC-White Paper_V4.pdf [https://perma.cc/Z8XV-BRR9] ("In at least 47 cases since 2002, the FTC has cited companies for failing either to design or to implement an appropriately comprehensive privacy or data security program. Almost all of these cases have been settled. The settlement requirements include relatively standardized language outlining the parameters of a data security program and begin to chart a path toward the development of similarly standard language for privacy programs. However, aside from requiring the designation of an adequately trained chief data security or privacy officer and the undertaking of regular risk assessments, the standard language that the FTC uses is terse and offers little in the way of specifics about the components of a compliance program. Consequently, anyone seeking to design a program that complies with FTC expectations would have to return to the complaints to parse out what the FTC views as '*un*reasonable'—and, by negation, reasonable—privacy and data security procedures.").

59. Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/VN7M-KW4T].

The FTC now bakes these basic precepts into its settlements.[60] While some argue that reasonableness requires examination of what the FTC, FCC, or even other states require,[61] defining reasonableness by looking at what is "unreasonable" provides little meaningful standards on which a business can rely and harkens to a "know it when I see it" standard.[62] Still, though, some argue that evaluating unreasonableness is the proper standard to apply to the CCPA.[63]

On the other hand, recommendations by the California Attorney General relating to privacy laws that predate the CCPA seem to favor a heightened, cybersecurity professional standard.[64] The Attorney General released a California Data Breach Report in February 2016, making five recommendations to organizations and state policymakers regarding data security.[65] Specifically, the Attorney General recommended:

60. Lesley Fair, *$575 Million Equifax Settlement Illustrates Security Basics for Your Business*, FTC (July 22, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/575-million-equifax-settlement-illustrates-security-basics?utm_source=govdelivery [https://perma.cc/SY2K-4DRL] ("The Equifax settlement is a study in how basic security missteps can have staggering consequences. Here are some tips other companies can take from the case—and we didn't have to look far for advice. The quotes are all from the FTC's brochure, *Start with Security*.").

61. Paige M. Boshell, *The* LabMD *Case and the Evolving Concept of "Reasonable Security,"* ABA Business Law Today (July 16, 2018), https://businesslawtoday.org/2018/07/labmd-case-evolving-concept-reasonable-security/ [https://perma.cc/4VPK-2NZN] (noting the statutory and regulatory approaches of other states' regulatory schemes, including California, Massachusetts, and Alabama).

62. Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

63. Mike Davis, *Cybersecurity Risk, What Does a "Reasonable" Posture Entail and Who Says So?*, Alliant Cybersecurity Blog (Apr. 3, 2019), https://www.rgcybersecurity.com/cybersecurity-risk-reasonable-posture/ [https://perma.cc/2WB7-K5UP] ("Given the absence of an exact definition of what 'reasonable' security practices entails, a simpler approach is to instead evaluate what constitutes a lack of reasonable security."); Boshell, *supra* note 62 ("Accordingly, the specific 'lessons learned' are often a list of 'do-nots.'").

64. *See Dissenting Statement of Commissioner Mignon L. Clyburn*, FCC, http://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0301/FCC-17-19A2.pdf [https://perma.cc/2JAX-AUZP] ("Both agencies require only reasonable data security measures, with caveats for the sensitivity of the data, size of the company and technical feasibility."); *see also* Jedidiah Bracy, *FCC Votes to Halt Wheeler-era Data Privacy Rule*, IAPP: Privacy Tracker (Mar. 2, 2017), https://iapp.org/news/a/fcc-votes-to-halt-wheeler-era-data-privacy-rule/ [https://perma.cc/AE5K-MK9V] ("Set to take effect Thursday, March 2, the rule would have required internet service providers to implement reasonable data security around consumer data, including Social Security numbers, browsing history, and geolocation data.").

65. 2016 Breach Report, *supra* note 7, at v ("The legal obligations to secure personal information include an expanding set of laws, regulations, enforce-

1) The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet.[66] The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security.
2) Organizations should make multi-factor authentication available on consumer-facing on-line accounts that contain sensitive personal information. This stronger procedure would provide greater protection than just the username-and-password combination for personal accounts such as online shopping accounts, health care websites and patient portals, and web-based email accounts.
3) Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers. This is a particular imperative for health care, which appears to be lagging behind other sectors in this regard.
4) Organizations should encourage individuals affected by a breach of Social Security numbers or driver's license numbers to place a fraud alert on their credit files and make this option very prominent in their breach notices. This measure is free, fast, and effective in preventing identity thieves from opening new credit accounts.

---

ment actions, common law duties, contracts, and self-regulatory regimes. California's information security statute requires businesses to use 'reasonable security procedures and practices . . . to protect personal information from unauthorized, access, destruction, use, modification, or disclosure.' . . . . Authoritative security standards describe the measures that organizations should take to achieve an appropriate standard of care for personal information.").

66. The Center for Internet Security Controls breaks down its 20 Controls into three topics: Basic Controls, Foundational Controls, and Organizational Controls. The "20 Controls" are: Basic CIS Controls (Inventory and Control of Hardware Assets; Inventory and Control of Software Assets; Continuous Vulnerability Management; Controlled Use of Administrative Privileges; Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers; and Maintenance, Monitoring and Analysis of Audit Logs); Foundational CIS Controls (Email and Web Browser Protections; Malware Defenses; Limitation and Control of Network Ports, Protocols and Services; Data Recovery Capabilities; Secure Configuration for Network Devices, such as Firewalls, Routers and Switches; Boundary Defense; Data Protection; Controlled Access Based on the Need to Know; Wireless Access Control; and Account Monitoring and Control); Organizational CIS Controls (Implement a Security Awareness and Training Program; Application Software Security; Incident Response and Management; and Penetration Tests and Red Team Exercises). *The 20 CIS Controls & Resources*, Ctr. for Internet Security, https://www.cisecurity.org/controls/cis-controls-list/ [https://perma.cc/M6K3-TPRB].

5) State policy makers should collaborate to harmonize state breach laws on some key dimensions. Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections, and retaining jurisdictional expertise.[67]

Thus, some erroneously conclude that the CCPA's reasonableness standard "derives" from the CISC standards set forth in the Report.[68] Not so. The Attorney General cannot legislate a standard of care by "recommendation," and even the Report itself recognizes its limitations as an "informational" document only.[69] And, the CCPA, rather than adopting the Report, called on the Attorney General to issue actual new regulations identifying reasonable procedures and practices through a proper administrative process. Finally, the California Legislature rejected a one-size-fits-all rule—like that proposed by the Attorney General's Report—that would have required adoption of the NIST standards.[70] While it was uncertain

67. 2016 Breach Report, *supra* note 7, at v–vi.

68. Divya Gupta & Cody Wamsley, *CCPA Requires "Reasonable Security": But You Can't have Reasonable Security Without Proper Vulnerability Management*, Dorsey & Whitney LLP (Sept. 12, 2019), https://www.dorsey.com/newsresources/publications/client-alerts/2019/09/ccpa-requires-reasonable-security [https://perma.cc/GQZ5-YZ8N] ("Managing or mitigating risk, however, requires implementing 'reasonable security,' which derives from the Center for Internet Security's Top 20 Critical Security Controls (CSC 20) per then California Attorney General in 2016, Kamala Harris.").

69. *Id.* ("This document is for informational purposes and should not be construed as legal advice or as policy of the State of California."); *see also supra* note 8 and accompanying text.

70. *Personal Information: Data Breaches, Hearing on A.B. 1035 Before the Assemb. Comm. on Privacy & Consumer Prot.*, 2019–2020 Leg., Reg. Sess. 1 (Cal. 2019) ("This bill [A.B. 1035] would require a person, business, or agency that owns or licenses computerized data that includes personal information (PI) to disclose a breach of the system within 45 days, as specified, and would further define 'reasonable security procedures and practices' for the purposes of California's Data Breach Notification Laws (DBNL). Specifically, this bill would: . . . 2) Provide, for the purposes of the DBNL and the limited private right of action in the California Consumer Privacy Act of 2018 (CCPA), that 'reasonable security procedures and practices' include, but are not limited to, a cybersecurity program that reasonably conforms to the current version, or a version that has been revised within the one-year period before the date of a security breach, of any of the following: [(1)] The Framework for Improving Critical Infrastructure Cyber Security developed by the National Institute of Standards and Technology (NIST). [(2)] NIST Special Publication 800-171."); *see also* Andy Green, *California Consumer Privacy Act (CCPA) Compliance Guide*, Veronis (Oct. 18, 2019), https://www.varonis.com/blog/california-consumer-privacy-act-ccpa/ [https://perma.cc/BV68-ERDB] ("AB-1035 takes on the challenge of defining the well-known boilerplate phrase 'reasonable security,' which is often found in state data breach laws but typically with no explanation attached to it mean-

whether the Attorney General would issue regulations before the CCPA's January 2020 effective date,[71] the Attorney General issued proposed regulations on October 4, 2019—none of which dealt with or clarified the reasonable policies and procedures standard of the CCPA.

Finally, European cybersecurity standards cannot be ignored either, particularly since commentators frequently refer to the CCPA as the California-version of General Data Protection Regulation (GDPR).[72] Europe's GDPR, passed in 2018, "has a very similar standard, requiring data controllers and processors to implement 'appropriate' technical, physical and administrative controls to protect personal information,"[73] but does not define "appropriate" or provide guidance as to its practical application. Article 5(1)(f) of the GDPR establishes the security principle, communicating that personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or

ing. This amendment boldly proposes the NIST Framework for Improving Critical Infrastructure Cybersecurity (CIS) and another NIST standard 800-171, which is a trimmed-down version of the encyclopedic 800-53, as a potential baseline security standard for the state. This is a big deal: not even the EU GDPR explicitly refers to outside data standards. Alas this amendment proved to be too radical for California: the CCPA was finalized on September 13, and the bill doesn't include this particular amendment. Oh well. Let's give California credit for considering the CIS Framework. In case you've forgotten, a framework is not the same as a security standard. Instead, it's a kind of meta-standard, which provides a list of meta-security controls that map into real security controls within existing data standards."); David Stauss, Erik Dullea, & Ephraim Hintz, *CCPA: Proposed Bill Would Link Reasonable Security to NIST Standards*, Byte Back (May 7, 2019), https://www.bytebacklaw.com/2019/05/ccpa-proposed-bill-would-link-reasonable-security-to-nist-standards/ [https://perma.cc/HUY4-Z88E] ("AB 1035's use of the phrase 'include, but are not limited to' and its omission of the CIS Controls from the enumerated list of conforming programs is likely to create confusion and risk for organizations that invested resources to abide by the Attorney General Office's guidance. The bill's narrow focus on NIST also ignores that there are other information security standards—such as ISO27001—that are routinely used by organizations to demonstrate information security compliance. By comparison, when Ohio recently created a safe harbor for certain data breach-related claims it included not only NIST standards but also the CIS Controls and ISO2700 family, among others.").

71. Khoury, *supra* note 5.

72. Geert Somers & Liesa Boghaert, *The California Consumer Privacy Act and the GDPR: Two of a Kind?*, Financier Worldwide (Nov. 2018), https://www.financierworldwide.com/the-california-consumer-privacy-act-and-the-gdpr-two-of-a-kind#.XWmlm8t8Cuk [https://perma.cc/2LB5-2BB7].

73. Phillip N. Yannella, *What Does "Reasonable" Data Security Mean, Exactly?*, CyberAdviser (July 20, 2018), https://www.cyberadviserblog.com/2018/07/what-does-reasonable-data-security-mean-exactly/ [https://perma.cc/T3EE-8PQH].

unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures ('integrity and confidentiality')."[74] Article 32 expands upon Article 5(1)(f) to set out what the security principle actually requires, namely taking account of "appropriate technical and organisational measures to ensure a level of security that is appropriate to the level of prevailing security risk[.]"[75] "The duty of security should reasonably include the continuum of applicable risks, from accidents and negligence at one end of the continuum to deliberate and malevolent actions at the other."[76]

Thus, it is clear from the CCPA's legislative hearing and its adoption of the CRA's reasonable security procedures and practices standard that the CCPA was meant to incorporate tort law's flexible reasonableness standard.[77] The courts interpreting the CRA and regulators interpreting other statutory cybersecurity schemes seem to reject a one-size-fits-all rule in favor of saying when cybersecurity procedures are *un*reasonable.[78] So, too, has the American Bar Association in its ethical guidelines for attorneys. Formal Opinion 477, which clarifies law firms' cybersecurity obligations, "rejects requirements for specific security measures, and instead adopts a 'reasonable' standards approach to deal with complex technical issues."[79]

74. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 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) para 173, ch. 2, art. 5(1)(f); *id.* at para 39 ("Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing.").

75. *Id.* at para 173, ch. IV § 2, art. 32.

76. Stuart Room, *Security of Personal Data*, *in* European Data Protection: Law and Practice 173 (2018).

77 *Hearing on A.B. 1950, supra* note 49.

78. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 254–55 (3d Cir. 2015); LabMD, Inc. v. FTC, 894 F.3d 1221, 1226 (11th Cir. 2018); *see also* Graves & McManus, *supra* note 4 (pointing out the FTC has not specified what constitutes "reasonable scrutiny," though lawyers have been asking that question for decades); Bailin, *supra* note 59, at 1 (stating the FTC offers little information as to how to comply with privacy programs).

79. Paul Gupta, *What is "Reasonable" Under the ABA's New Cybersecurity Obligations for Law Firms?*, Thompson Reuters (July 12, 2017), http://www.legalexecutiveinstitute.com/aba - new - cybersecurity - obligations/ [https://perma.cc/K6EN-HTTA]. The ABA Committee on Ethics and Professional Responsibility concluded a reasonable efforts standard:

> rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to

Specifically, law firms must create and maintain their own "reasonable measures" and "fact-based analysis" to assess and mitigate risks in order to understand the nature of the threat; understand how client confidential information is transmitted and where it is stored; understand and use reasonable electronic security measures; determine how electronic communications about clients' matters should be protected; label client confidential information; and train lawyers and non-lawyer personnel in technology and information security.[80] "Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a 'reasonable efforts' determination."[81] Those factors include:

> the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[82]

In other words, rather than adopting requirements for specific security measures, as advocates for a technical security-based approach would do with respect to the CCPA, the ABA adopts a process-based approach that recognizes a historic familiarity that ABA members would have with reasonableness as a legal term.

Thus, a few guidelines do appear. First, as stated above, reasonableness remains the CCPA's standard. Second, a cybersecurity breach can still happen notwithstanding the maintenance of reasonable security procedures adapted to avoid the breach.[83] Third, the mere fact of the breach by itself does mean that business's cybersecurity procedures were unreasonable.[84] Fourth, the existence of higher quality or state-of-the-art security measures is insufficient by itself to demonstrate that a business's procedures were unreasonable.[85] Fifth, the absence of any security procedures, of any person trained in privacy of cybersecurity, and of regular risk assessments repre-

---

> those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 477, at 4 (2017) [hereinafter ABA Formal Op. 477].

80. ABA Formal Op. 477, *supra* note 79, at 5–8.

81. *Id*. at 4.

82. *Id*.

83. *In re* Twitter, Inc., 2011 WL 914034, at *19 (F.T.C. Mar. 2, 2011) (stating that just because a breach occurred, does not mean there were not reasonable security procedures in place).

84. Anderson v. Kimpton Hotel & Rest. Grp., LLC, Case No. 19-cv-01860-MMC, 2019 WL 3753308, at *5–6 (N.D. Cal. Aug. 8, 2019).

85. Razuki v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018).

sent a common theme underlying a finding of unreasonableness.[86] And, finally, reasonableness always requires some balancing: the level of security must be appropriate to the risk and the cost of additional safeguards.[87]

B. "Reasonable" Means What It Says.

1. The CCPA's common law roots.

a. Foreseeability and risk/utility.

As stated above, the CCPA's roots are grounded in reasonableness, which derive from common law negligence,[88] and is a term well-established in California common law.[89] The CCPA's use of the term reasonableness can-

86. *See* Room, *supra* note 76, at 173.

87. *Id.* at 173 ("The duty of security should reasonably include the continuum of applicable risks, from accidents and negligence at one end of the continuum to deliberate and malevolent actions at the other.").

88. Judicial Council of Cal., Civil Jury Instructions, CACI No. 400 (2019) [hereinafter Cal. Jury Instructions] ("To establish this claim, [plaintiff] must prove all of the following: 1. That [defendant] was negligent; 2. That [plaintiff] was harmed; and 3. That [defendant]'s negligence was a substantial factor in causing [plaintiff]'s harm."). The *Rowland* Court

> identified several considerations that, when balanced together, may justify a departure from the fundamental principle embodied in Civil Code section 1714: 'the foreseeability of harm to the plaintiff, the degree of certainty that the plaintiff suffered injury, the closeness of the connection between the defendant's conduct and the injury suffered, the moral blame attached to the defendant's conduct, the policy of preventing future harm, the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach, and the availability, cost, and prevalence of insurance for the risk involved.' . . . "The concept of foreseeability of risk of harm in determining whether a duty should be imposed is to be distinguished from the concept of '"foreseeability" in two more focused, fact-specific settings' to be resolved by a trier of fact. 'First, the [trier of fact] may consider the likelihood or foreseeability of injury in determining whether, in fact, the particular defendant's conduct was negligent in the first place. Second, foreseeability may be relevant to the [trier of fact's] determination of whether the defendant's negligence was a proximate or legal cause of the plaintiff's injury.'

Id. at CACI No. 400 annot., pp. 222–23 (citations omitted).

89. *Id.* at CACI No. 401 ("Negligence is the failure to use reasonable care to prevent harm to oneself or to others. A person can be negligent by acting or by failing to act. A person is negligent if he or she does something that a reasonably careful person would not do in the same situation or fails to do something that a reasonably careful person would do in the same situation. You must decide how a reasonably careful person would have acted in [name of plaintiff/defendant]'s situation.").

not be ignored.[90] By using this term, the CCPA incorporated decades of legal principles of reasonableness in negligence law that have been well-established in other contexts.[91]

"The duty is of ordinary care under all the circumstances, and it varies with changing circumstances. The standard is that of the 'ordinary prudent or reasonable person.'"[92]

> Due care requires the avoidance of any 'unreasonable risk,' which means any 'unduly dangerous conduct.' The basic question of whether the risk of danger to others outweighs the utility of the act or the manner in which it is done; if so, the risk is unreasonable and the act is negligent. . . . Conduct is negligent where some unreasonable risk of danger to others would have been foreseen by a reasonable person.[93]

In some ways, cybersecurity can be analogized to the duty to anticipate criminal behavior by computer hackers, thieves, or ramsomers,[94] based on whether a special relationship was created,[95] or by the types of data held.[96]

---

90. *See Hearing on A.B. 1950*, *supra* note 48.
91. Razuki v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 6018361, at *1–2 (S.D. Cal. Nov. 15, 2018).
92. 6 B. E. Witkin et al., Summary of California Law § 998 (11th ed. 2019).
93. *Id*. § 999 (citations omitted).
94. *See* Cal. Jury Instructions, *supra* note 88, at CACI No. 400, annot., p. 224 ("[Defendant] relies on the rule that a person has no general duty to safeguard another from harm or to rescue an injured person. But that rule has no application where the person has caused another to be put in a position of peril of a kind from which the injuries occurred." (quoting Carlsen v. Koivumaki, 174 Cal. Rptr. 3d 339, 345 (Cal. Ct. App. 2014))).
95. *Id*. ("Typically, in special relationships, 'the plaintiff is particularly vulnerable and dependent upon the defendant who, correspondingly, has some control over the plaintiff's welfare. . . . A defendant who is found to have a 'special relationship' with another may owe an affirmative duty to protect the other person from foreseeable harm, or to come to the aid of another in the face of ongoing harm or medical emergency." (quoting *Carlsen*, 174 Cal. Rptr. 3d at 353–54)).
96. Dittman v. UPMC, 196 A.3d 1036, 1048 (Pa. 2018) ("Again, Employees allege that UPMC, their employer, undertook the collection and storage of their requested sensitive personal data without implementing adequate security measures to protect against data breaches, including encrypting data properly, establishing adequate firewalls, and implementing adequate authentication protocol. The alleged conditions surrounding UPMC's data collection and storage are such that a cybercriminal might take advantage of the vulnerabilities in UPMC's computer system and steal Employees' information; thus, the data breach was 'within the scope of the risk created by' UPMC. Therefore, the criminal acts of third parties in executing the data breach do not alleviate UPMC of its duty to protect Employees' personal and financial information from that breach.") (citation omitted); *see also id*. at 1057 (Saylor, C.J., concurring in part) ("Ultimately, I find that an employer who collects confidential personal and financial information from employees stands in such a special relationship to

In the absence of a special relationship, however, criminal behavior traditionally constitutes a supervening cause,[97] unless the defendant's conduct created the specific situation that invited the criminal to take advantage of it.[98] While the CCPA imposes many obligations on controllers, processors, and vendors of consumer data, nothing in the CCPA suggests or creates a special relationship such as the types traditionally recognized.

Still other analogies exist, such as the law surrounding bailments or premises liability. As to the former, the duty of care in bailment situations

---

those employees with respect to that information, and I have no difficulty concluding that such a relationship should give rise to a duty of reasonable care to ensure the maintenance of appropriate confidentiality as against reasonably foreseeable criminal activity.").

97. California adheres to the modern view exemplified in section 448 of the Restatement Second of Torts:

> 'The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although the actor's negligent conduct created a situation which afforded an opportunity to the third person to commit such a tort or crime, unless the actor at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime.' Present California decisions establish that a criminal act will be deemed a superseding cause unless it involves a particular and foreseeable hazard inflicted upon a member of a foreseeable class.
>
> [A]n intervening act does not amount to a 'superseding cause' relieving the negligent defendant of liability if it was reasonably foreseeable: '[An] actor may be liable if his negligence is a substantial factor in causing an injury, and he is not relieved of liability because of the intervening act of a third person if such act was reasonably foreseeable at the time of his negligent conduct.' Moreover, under section 449 of the Restatement Second of Torts that foreseeability may arise directly from the risk created by the original act of negligence: 'If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act whether innocent, negligent, intentionally tortious, or criminal does not prevent the actor from being liable for harm caused thereby.'

Cal. Jury Instructions, *supra* note 88, at CACI No. 433, annot., pp. 296–97 (first quoting Kane v. Hartford Accident & Indemnity Co., 159 Cal. Rptr. 446, 451 (Cal. Ct. App. 1979); then quoting Landerous v. Flood, 551 P.2d 389, 395 (Cal. 1976)).

98. *Id.* at p. 297 (commenting CACI No. 433 erroneously allowed a defendant to assert "a complete defense based on a heightened standard of foreseeability inapplicable to plaintiffs' design defect claims" (quoting Collins v. Navistar, Inc., 155 Cal. Rptr. 3d 137, 157 (Cal. Ct. App. 2013)); *see also* Williams v. Fremont Corners, Inc., 250 Cal. Rptr. 3d 46, 53 (Cal. Ct. App. 2019) ("[D]uty in such circumstances is determined by a balancing of 'foreseeability' of the criminal acts against the 'burdensomeness, vagueness, and efficacy' of the proposed security measures.").

would be premised on the assumption that data is "property" that can be the subject of the bailment.[99] If so, bailments give rise to three duties of care. In a gratuitous bailment for the sole benefit of the bailor, the duty is of slight care.[100] Where the bailment is for the benefit of both parties, the duty is of ordinary care. Where the bailment is for the sole benefit of the bailee, the duty is one of great care.[101] Bailment liability may be enlarged or constricted by contract.[102]

> A Bailee for hire is not an insurer of the safety of goods. The Bailee must use ordinary care, i.e., such care as an ordinarily prudent person exercises with respect to his or her own property of a similar description. The standard varies with the time and place and is influenced by the custom and usage of business.[103]

As to the latter, a premises liability analogy may work in some circumstances, such as when retailers "invite" consumers to "visit" their websites,

99. *See* Atul Singh, *Protecting Personal Data as a Property Right*, India L. Inst. L. Rev., Winter 2016, at 123, 123, http://ili.ac.in/pdf/p9_atul.pdf [https://perma.cc/7BY7-HU8A] ("Another approach being considered is treatment of personal data as an incorporeal property and its protection likewise."); Steven Hill, *Should Big Tech Own Our Personal Data?*, Wired (Feb. 13, 2019), https://www.wired.com/story/should-big-tech-own-our-personal-data/ [https://perma.cc/UVC2-FMBN] ("That's because our personal data is not merely a form of individual property. Increasingly, it's a core part of our personhood, following us throughout our lives. Personal control over our own data ought to be regarded as a human right that cannot be taken or given away."). Contrariwise, insurance carriers have posited that loss of pure data is not "property damage." *See* Am. Online, Inc. v. St. Paul Mercury Ins. Co., 347 F.3d 89, 96 (4th Cir. 2003) (upholding denial of claim for damage to computer's data from software finding no physical damage to tangible property); Ward Gen. Ins. Servs., Inc. v. Emp'rs Fire Ins. Co., 7 Cal. Rptr. 3d 844, 850 (Cal. Ct. App. 2003) ("[I]nformation is stored in a physical medium . . . but the information itself remains intangible. [Here,] Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored *information*."); State Auto Prop. & Cas. Ins. Co. v. Midwest Computs. & More, 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001) ("Alone, computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property."); *see also* Mobley v. State, No. S18G1546, 2019 WL 5301819, at *6 (Ga. Oct. 21, 2019) (finding the retrieval of data without a warrant at the scene of a collision was a search and seizure that implicated property rights the Fourth Amendment). *See generally* Angelique Carson, *US Lawmakers Consider Whether Your Data Should Be a 'Property Right,'* IAPP: The Privacy Advisor (Oct. 25, 2019), https://iapp.org/news/a/us-lawmakers-consider-whether-your-data-should-be-a-property-right/ [https://perma.cc/5GNK-NFKP] (reviewing recent congressional hearings discussing the potential economic value of personal data as a property right).

100. 13 Witkin et al., *supra* note 92, § 167.

101. *Id.*

102. *Id.* § 168.

103. *Id.* § 169.

in the figurative sense, and to provide data.[104] "Broadly speaking, premises liability presupposes that a defendant property owner allowed a dangerous condition on its property or failed to take reasonable steps to secure its property against criminal acts by third parties."[105]

> It must also be emphasized that the liability imposed is for negligence. The question is whether in the management of his property, the possessor of land has acted as a reasonable person under all the circumstances. The likelihood of injury to plaintiff, the probable seriousness of such injury, the burden of reducing or avoiding the risk, the location of the land, and the possessor's degree of control over the risk-creating condition are among the factors to be considered by the trier of fact in evaluating the reasonableness of a defendant's conduct.[106]

b. Cybersecurity does not justify varying from the reasonableness principles that the CCPA incorporates.

Because the CCPA is grounded in tort principles, the reasonable procedures and practices standard should balance the burden of precaution against the foreseeability of injury to the data subjects and nature of the data held, and the data controller's and processor's degree of control over the risk, if any.[107] Some, however, have argued that cybersecurity is differ-

104. Cal. Jury Instructions, *supra* note 88, at CACI No. 1001 (stating a property owner "is negligent if [they] fail[] to use reasonable care to keep the property in a reasonably safe condition. [They] must use reasonable care to discover any unsafe conditions and repair, replace, or give adequate warning of anything that could be reasonably expected to harm others.").

105. *Id.* at annot., p. 604 (quoting Delgado v. Am. Multi-Cinema, Inc., 85 Cal. Rptr. 2d 838, 840 n.1 (Cal. Ct. App. 1999)).

106. *Id.* at annot., p. 606 (quoting Sprecher v. Adamson Co., 636 P.2d 1121, 1128–29 (Cal. 1981)); *see also* Restatement (Second) of Torts § 344 cmt. f (Am. Law Inst. 1965) ("Since the possessor is not an insurer of the visitor's safety, he is ordinarily under no duty to exercise any care until he knows or has reason to know that the acts of the third person are occurring, or are about to occur. He may, however, know or have reason to know, from past experience, that there is a likelihood of conduct on the part of third persons in general which is likely to endanger the safety of the visitor, even though he has no reason to expect it on the part of any particular individual. If the place or character of his business, or his past experience, is such that he should reasonably anticipate careless or criminal conduct on the part of third persons, either generally or at some particular time, he may be under a duty to take precautions against it, and to provide a reasonably sufficient number of servants to afford a reasonable protection.").

107. United States v. Carrol Towing Co, 159 F.2d 169, 173 (2d Cir. 1947) (Hand, J.) ("Since there are occasions when every vessel will break from her moorings, and since, if she does, she becomes a menace to those about her; the owner's duty, as in other similar situations, to provide against resulting injuries is a function of three variables: (1) The probability that she will break away; (2) the gravity of the resulting injury, if she does; (3) the burden of adequate precau-

ent, that the "risk/utility" test of "reasonableness" is inadequate with respect to establishment of cybersecurity procedures,[108] and that precedent with regard to the constantly evolving rules of data protection, cybersecurity, and cyber-breach should evolve slowly and with caution.[109] But commentators critical of the CCPA's negligence standard fail to demonstrate why the CCPA's use of traditional negligence principles is unable to provide adequate rules for data protection, cybersecurity, and data breach. A technical security-based, non-legal standard for reasonableness improperly conflates state-of-the-art cybersecurity techniques with a legal standard of negligence that requires only that a business have reasonable procedures and practices.[110] In other words, such a heightened standard improperly conflates negligence's "reasonable person" standard with a "professional cyber-security" standard.[111]

In assessing foreseeability, tort law analyzes the "general character of the event or harm . . . not its precise nature or manner of occurrence."[112] So, in the context of data breaches, some measure of foreseeability of risk necessarily will always exist.[113] Some data security experts have quipped therefore that there are only two types of companies: "those that have been hacked and those that don't know they've been hacked."[114] Reasonableness

tions. Possibly it serves to bring this notion into relief to state it in algebraic terms: if the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P: i.e., whether $B < PL$.").

108. Davis, *supra* note 63 (identifying reasons for the underlying problem of establishing a set duty of care to cybersecurity as "the ever-changing cyber threat landscape and the fact that each data breach is unique").

109. Todd Rowe, *Recent Case Sheds Light on What Courts May Find Makes Security Measures Reasonable*, Privacy Risk Report (Jan. 19, 2017), https://privacyriskreport.com/recent-case-sheds-light-on-what-courts-may-find-makes-security-measures-reasonable/ [https://perma.cc/A5T7-KPT9].

110. *See* Stan, supra note 8 (stating there is no current "legal definition for what constitutes appropriate reasonable security procedures and policies").

111. Kang, *supra* note 9.

112. Kesner v. Super. Ct., 384 P.3d 283, 292 (Cal. 2016).

113. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 Berkeley Tech. L.J. 1553, 1570 (2005) ("In a networked world, it is reasonably foreseeable that computer hackers or cybercriminals will discover and exploit known vulnerabilities in operating systems.").

114. Storm v. Paytime, Inc., 90 F. Supp. 3d 359, 360 (M.D. Pa. 2015) (quoting Nicole Perlroth, *The Year in Hacking, by the Numbers*, N.Y. TIMES (Apr. 22, 2013), http://bits.blogs.nytimes.com/2013/04/22/the-year-in-hacking-by-the-numbers/?_r=0 [https://perma.cc/FM7D-J5TF]). A similar quip has been recited for motorcycle riders, but that is no basis for imposing comparative negligence simply for lawfully operating a motorcycle. u/Feyree, *"There's Two Types of Riders; Those Who Have Crashed, and Those Who Will*," Reddit (Apr. 18, 2016), https://www.reddit.com/r/motorcycles/comments/4gt4ub/theres_two_types_of_riders_those_who_have_crashed/ [https://perma.cc/JPR6-F5ZX] ("I've heard this saying a lot. I'm just next weekend getting my provisional

in data breach cases, however, must look at whether a business was on notice of a *particular* risk or vulnerability—rather than generally knowing that cybercriminals exist.[115] To establish this more tailored foreseeability, a trier of fact could evaluate prior instances of "security breaches, intrusions, or virus incidents."[116] Doing so would safeguard against foreseeability being overstated in hindsight.[117]

---

motorcycle licence. I am comfortable accepting the risk of broken bones, but the possibility for permanent injuries is discouraging. I will do all I can to minimize my risk, including full protective gear and defence driving. However, I'm still worried about the risk of more serious injuries. Is this activity worth the risk of the potential loss of all my other activities?").

115. Rustad & Koenig, *supra* note 113, at 1583.

116. *Id.* at 1584. *Compare* Castillo v. Seagate Tech., LLC, No. 16-cv-01958-RS, 2016 WL 9280242, at *6 (N.D. Cal. Sep. 14, 2016) ("Nonetheless, plaintiffs cannot show the harm they suffered was foreseeable or that Seagate is morally culpable in this ordeal. Plaintiffs insist this data breach was foreseeable because an Internet security research firm wrote an article about the sort of phishing scam to which Seagate fell prey. . . . [P]laintiffs here have not provided any information about whether Seagate was aware of this article or knew about similar data breaches. Plaintiffs also have not provided enough information to permit an inference that Seagate should have been on the lookout for fraudulent requests for W-2 information."), *with* Corona v. Sony Pictures Entm't, Inc., No. 14-CV-09600 RGK (Ex), 2015 WL 3916744, at *2 (C.D. Cal. June 15, 2015) (data breach and resulting injury to former employees were foreseeable because the defendant had been the victim of similar phishing attacks in the past and was aware of similar breaches at other companies); *see also In re* Brinker, Case No. 3:18-cv-686-J-32MCR, 2019 WL 3502993, at *2 (M.D. Fla. Aug. 1, 2019) ("'Given the numerous reports indicating the susceptibility of POS systems and consequences of a breach, Brinker was well-aware, or should have been aware, of the need to safeguard its POS systems.' Plaintiffs allege that despite this knowledge, Brinker failed to comply with industry standards for information security, including the Payment Card Industry Data Security Standard ("PCI DSS"). And, 'Brinker failed to implement adequate data security measures to protect its POS networks from the potential danger of a data breach and failed to implement and maintain reasonable security procedures and practices. . . .' Specifically, 'Brinker operated POS systems with outdated operating systems and software; failed to enable point-to-point and end-to-end encryption; and, failed to take other measures necessary to protect its data network.'") (citations omitted).

117. Meiring de Villiers, *Reasonable Foreseeability in Information Security Law: A Forensic Analysis*, 30 Hastings Comm. & Ent. L.J. 419, 477 (2008) ("Research in behavioral psychology suggests, for instance, that people tend to overstate the predictability of past events, and that after-the-fact decisions by judges and juries about what an individual knew or should have known may be influenced by knowledge of what actually occurred."); *see also* Razuki v. Caliber Home Loans, Inc., Case No. 17cv1718-LAB (WVG), 2018 WL 6018361, at *1 (S.D. Cal. Nov. 15, 2018) ("[S]imply knowing of higher-quality security measures is not sufficient to state a claim.").

The CCPA's "appropriate to the nature of the information" clause does not change the inquiry.[118] More likely, however, the term merely suggests that the specialty of the data that a business collects may affect the type and extent of the security measures and procedures a business must implement.[119] But the qualifying language does not change the CCPA's requirement that those procedures and practices be reasonable. For example, the standard for operating an automobile must always be reasonable, despite the fact that what is reasonable may vary depending on good or adverse driving conditions. Thus, reasonableness under certain circumstances, with respect to handling sensitive data,[120] may require a controller or processor to "slow down"—to continue the metaphor—and take additional precautions, such as encryption, pseudonymizing data, or anonymizing data.[121] The measures and procedures under the CCPA must still, however, be reasonable.[122]

Given that cyber-crime and information security are constantly moving targets, and that the CCPA's private right of action for data breach only

118. This language could suggest that the nature of the data may require different readability treatment, with data encryption running the spectrum from none/unencrypted to pseudonymous to anonymous/encrypted.

119. Brennan v. Cockrell Invest., Inc., 111 Cal. Rptr. 122, 125 (Cal. Ct. App. 1973) ("Possession means control, or at least some considerable degree of it.").

120. Matt Wes, *Looking to Comply with GDPR? Here's a Primer on Anonymization and Pseudonymization*, IAPP: The Privacy Advisor (Apr. 25, 2017), https://iapp.org/news/a/looking-to-comply-with-gdpr-heres-a-primer-on-anonymization-and-pseudonymization/ [https://perma.cc/34TJ-2FSH] (discussing two distinct techniques, anonymization and pseudonymization "that permit data controllers and processors to use de-identified data. The difference between the two techniques rests on whether the data can be re-identified"). There may come a day where all data must be encrypted as technology evolves to allow processing of data without encrypting the data. *Homomorphic Encription: A Guide to Advances in the Processing of Encrypted Data*, Thales (Mar. 11, 2016), https://www.thalesgroup.com/en/worldwide/security/news/homomorphic-encryption-guide-advances-processing-encrypted-data [https://perma.cc/ZXD7-H89A] ("[I]f we want to use that information . . . we must first decrypt it. And as soon as we do that the entire set of data becomes vulnerable to unauthorized access and theft.").

121. Gabe Maldoff, *Top 10 Operational Impacts of the GDPR: Part 8—Pseudonymization*, IAPP: The Privacy Advisor (Feb. 12, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-8-pseudonymization/ [https://perma.cc/J6R3-2ABE] (identifying pseudonymization as a new concept introduced by the GDPR, which separates "data from direct identifiers so that linkage to identity is not possible without additional information that is held separately").

122. *See* Solove & Schwartz, *supra* note 31 (endorsing a "reasonable safeguards approach" to data security because it is "open-ended and evolves as standards and best practices develop and as security threats change," yet wary that when "left to their own devices, organizations can interpret 'reasonable' in essentially unreasonable way").

attaches to the disclosure of highly sensitive information,[123] judicial decisions preceding the CCPA's enactment suggest that industry standards might determine what is a reasonable or appropriate security measure.[124] However, in the absence of regulations from the Attorney General clarifying what security procedures might be appropriate, businesses may overreact and adopt excessive precautions[125]—particularly because "[s]ecurity breaches are an inevitable byproduct of collecting sensitive" data.[126] Alternatively, while "evidence of custom or practice of others similarly situated is always admissible on the issues of due care and negligence," "a long line of California cases supports the general rule that custom, while relevant, is not conclusive on the issue; i.e., it cannot make due care out of conduct that is in fact negligent."[127] In other words, an industry standard on cybersecurity might be either too strict or too loose under the circumstances to evaluate whether a business acted reasonably.

Thus, it is not clear that industry standards always conclusively measure the reasonableness of a security procedure or practice.[128] Indeed, even industry organizations purporting to set threshold limits of cybersecurity cannot agree on a proper industry standard, sometimes engaging in cybersecurity one-upmanship that, in the end, little resembles a reasonable security procedure and practice.[129] Ultimately, "[t]he duty is of ordinary care under all the circumstances, and it varies with the changing circumstances."[130] Due care requires avoiding "any 'unreasonable risk,' which means 'unduly dangerous conduct.' The basic question is whether the risk of danger to others outweighs the utility of the act or the manner in which it is done; if so, the risk is unreasonable and the act is negligent."[131] The

123. Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. Cal. L. Rev. 241, 268 (2007); *see* Cal. Civ. Code § 1798.81.5(d)(1)(A) (providing what constitutes highly sensitive information).

124. *See, e.g.*, Hameed-Bolden v. Forever 21 Retail, Inc., Case No. CV 18-03019 SJO (JPRx), 2018 WL 6802818 (C.D. Cal. Oct. 1, 2018); *In re* Sony Gaming Networks, 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (finding the existence of a legal duty to protect customer's personal information was supported by common sense and California law).

125. Giuseppe Dari-Mattiacci, *Errors and the Functioning of Tort Liability*, 13 Sup. Ct. Econ. Rev. 165, 169, 186 (2005) (arguing uncertainty in liability rules could result in over-precaution).

126. Citron, *supra* note 123, at 264.

127. 6 Witkin, *supra* note 92, § 1029.

128. Some courts have assumed that an industry standard of care applies. Silverpop Sys. v. Leading Mkt. Techs., Inc., 641 F. App'x 849, 852 (11th Cir. 2016) ("[A]ssuming, *arguendo*, that Silverpop had a duty to conform its conduct to a particular standard to protect against incidents resulting in a data breach, LMT has failed to present evidence to establish the applicable standard of care.").

129. *See* FTC Comment on NIST, *supra* note 8, at 10–11.

130. 6 Witkin, *supra* note 92, at § 998.

131. *Id.* § 999.

burden of precautionary policies and practices should be measured alongside industry standards, but not dogmatically governed by them. A reasonableness analysis that considers the marginal utility of each level of cost of increased security—the financial and non-monetary burden to implement additional security procedures—provides the flexibility that tort law, and the concept of reasonableness, envisions. Moreover, tort law should provide predictability and the ability for businesses to comply with it, as other statutory schemes include reasonable policies and procedures.

2. Statutory analogies: "reasonable policies and procedures" defenses.

Courts have broad experience evaluating a business's "reasonable procedures" as a statutory defense to liability. Common threads of these reasonable policies and procedures or "commercially reasonable" defenses are that a business is not a guarantor against accidents and that a business need not employ state-of-the-art procedures to protect against them. Again, reasonableness is required.

The "maintenance of procedures reasonably adapted to avoid any such error" is a standard well established and explored, at least under federal law.[132] Under the Fair Debt Collections Practice Act (FDCPA), for example, a debt collector can avoid liability for a violation of the FDCPA if it establishes such "reasonable" procedures adapted to avoid violation. The Supreme Court in *Jerman v. Carlisle, McNellie, Rini, Kramer & Ulrich, L.P.A.*,[133] expounded on the term "procedure"—as contrasted to the CCPA's use of the term "security procedure"—

> The dictionary defines "procedure" as "a series of steps followed in a regular orderly definite way. " In that light, the statutory phrase is more naturally read to apply to processes that have mechanical or other such "regular orderly" steps to avoid mistakes—for instance, the kind of internal controls a debt collector might adopt to ensure its employees do not communicate with consumers at the wrong time of day, § 1692c(a)(1), or make false representations as to the amount of a debt, § 1692e(2).[134]

Liability does not arise "if reasonable procedures are place, even if the collector could have done more to avoid the error."[135]

---

132. 15 U.S.C §1692k(c) (2012). Similarly, under the Fair Credit Reporting Act, "[t]he FCRA does not require error free reports. Liability does not flow automatically from the mere fact that the CRA reports inaccurate information; instead, it must flow from its failure to follow reasonable procedures." Nat'l Consumer Law Ctr., Fair Credit Reporting 158-59 (9th ed. 2017) (citing 15 U.S.C. 1692e(b)).

133. Jerman v. Carlisle, McNellie, Rini, Kramer & Ulrich LPA, 559 U.S. 573 (2010).

134. *Id*. at 587 (citation omitted).

135. *E.g.*, Ross v. RJM Acquisitions Funding, LLC, 480 F.3d 493, 498 (7th Cir. 2007) (stating reasonable procedures are required, not "state of the art"); *see also* Nat'l Consumer Law Ctr., Fair Debt Collection 628 n.149 (9th ed. 2018) (citing decisions).

Similarly, the Uniform Commercial Code (UCC) contains a common theme that a business act in a "commercially reasonable fashion."[136] Again, this requirement does not make businesses guarantors against fraud. UCC section 4A-203, for example, requires commercially reasonable safeguards for electronic funds transfers[137] which "encourage(s) banks to institute reasonable safeguards against fraud but [does] not to make them insurers against fraud."[138]

> A security procedure is not commercially unreasonable simply because another procedure might have been better or because the judge deciding the question would have opted for a more stringent procedure. The standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank, which is a lower standard. On the other hand, a security procedure that fails to meet prevailing standards of good banking practice applicable to the particular bank should not be held to be commercially reasonable.[139]

Patco Construction Co. v. People's United Bank,[140] for example, explained:

> There are two ways by which a security procedure may be shown to be commercially reasonable. First is by reference to: [T]he wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer and security procedures in general use by customers and receiving banks similarly situated. The Article is explicit that "[t]he standard is not whether the security procedure is the best available. Rather it is whether the procedure is reasonable for the particular customer and the particular bank. . . ."[141]

The standard is similarly applied by the UCC for negotiable instruments, such as in forged maker cases. In such cases, a payor bank's liability is generally determined by standards set by comparable banks—not what state-of-the-art security procedures are available.[142]

---

136. *See, e.g.*, Cal. Com. Code § 1201(20), ("'Good faith,' . . . means honesty in fact and the observance of reasonable commercial standards of fair dealing.").
137. These standards have been explored fully elsewhere. *See generally* C. David Hailey, *What Is a Commercially Reasonable Security Procedure Under Article 4A of the Uniform Commercial Code?*, 21 Fidelity L.J. 95 (2015) (exploring the extent of bank liability under Article 4A when fraudulent funds are electronically transferred).
138. U.C.C. § 4A-203 cmt 4 (Am. Law Inst. & Unif. Law Comm'n 2012).
139. *Id.*
140. Patco Constr. Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012).
141. *Id.* at 209 (quoting U.C.C. § 4A-203 cmt. 4).
142. *See, e.g.*, Espresso Roma Corp. v. Bank of Am., 124 Cal. Rptr. 2d 549, 555 (Cal Ct. App. 2002) ("[N]either the Bank's own procedures, nor reasonable commercial standards, required that the bank sight review any of the forged checks.").

What constitutes a commercially reasonable security procedure under the UCC requires a case-by-case analysis or, stated in negligence terms, ordinary care under all the circumstances. But, unlike the CCPA, "commercial reasonableness" contains a modifier that the CCPA does not: that of "commercial" reasonableness; i.e. one that necessarily incorporates a "commercial" standard of care.[143] Thus, while reasonable policies and procedures or commercially reasonable defenses provide a good explanation why a business need not maintain state-of-the-art procedures nor be a guarantor against accidents, "commercially" reasonable standards may fail where they impose a commercial standard not required by the language of the CCPA.

IV. Conclusion

The bottom line is that the CCPA's "reasonable security procedures and practices" standard requires "reasonableness." Trial lawyers and judges have centuries of experience dealing with the requirement that persons and businesses act "reasonably." Of course, practitioners laudably advise their clients to undertake strict technical or professional cybersecurity policies and procedures to protect consumer data. But the CCPA's requirement that businesses undertake reasonable security procedures and practices in order to avoid catastrophic class action liability neither requires nor allows a business to act unreasonably. Courts and trial lawyers should resist the temptation to impose, in hindsight, a standard higher than reasonableness in order to foist catastrophic liability on a business under the CCPA.

The reasonable security procedures and practices language in the CCPA—and its companion, the CRA—was meant to incorporate tort law's reasonableness standard. There is no one-size-fits-all. The guidelines in determining what measures are *un*reasonable provide some guidance as to what is, in fact, reasonable. Yet, cybersecurity breaches unfortunately can still happen notwithstanding the maintenance of reasonable security procedures designed to avoid the breach. The mere fact of a cybersecurity breach or that better, state-of-the-art cybersecurity procedures exist is not, alone, conclusive evidence that a business failed to maintain reasonable cybersecurity procedures. Rather, reasonableness requires balancing: that the level of security be appropriate to the risk and appropriate to the nature of the information.

143. Hailey, *supra* note 137, at 131 ("[C]ourts have referred to the 2005 FFIEC Guidance as part of the analysis of the 'commercially reasonable' issue. . . . [T]he Guidance has become more significant in recent cases. . . . [And] will become more important as the fraudulent activity becomes more sophisticated and the security procedures become more complex.").