VOLUME 25 SUMMER 2020

ILLINOIS BUSINESS LAW JOURNAL

CONVENIENCE V. CONFIDENTIALITY: THE CALIFORNIA CONSUMER PRIVACY ACT AND THE LIMITS OF ITS PRIVATE RIGHT OF ACTION

❖ NOTE ❖

Zachary Read *

I. INTRODUCTION

The rapid development of 'emerging technologies,' such as IoT devices, has created a wealth of functional benefits for consumers and businesses alike.[1] Technology has created what people want most: convenience.[2] However, the countless conveniences created by new technologies have been accompanied by security and privacy concerns as well.[3] Companies such as Amazon have made retail transactions easier than ever for consumers by having products advertised according to personalized tastes and facilitated through efficient, 'one-click' purchases.[4] However, personal identifiers such as contact information, purchase history, and credit card information have also been exposed to data breaches.[5] While consumers want the benefits that Amazon's services provide, there is a growing concern over keeping personal information secure and private.[6] Regulatory bodies have struggled with

1. *See* James McArthur, *6 Ways On How Technology Has made Our Life Easier*, ENGADGET (Oct. 17, 2016), https://www.engadget.com/2016/10/17/6-ways-on-how-technology-has-made-our-life-easier/; Mehedi Hasan, *Top 20 Emerging IoT Trends That Will Shape Your Future Soon*, UBUNTUPIT, https://www.ubuntupit.com/top-20-emerging-iot-trends-that-will-shape-your-future-soon/.

2. J. Walker Smith, *Is the Convenience of Technology Worth the Security Risks?*, AMERICAN MARKETING ASSOCIATION (April 25, 2018), https://www.ama.org/marketing-news/is-the-convenience-of-technology-worth-the-security-risks/.

3. *See id.*

4. *See id.*

5. John E. Dunn, *Data of Millions of eBay and Amazon Shoppers Exposed*, NAKED SECURITY (Mar. 12, 2020), https://nakedsecurity.sophos.com/2020/03/12/data-of-millions-of-ebay-and-amazon-shoppers-exposed/

6. *See generally Public Opinion on Privacy*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/survey/

*J.D. Candidate, Class of 2022, University of Illinois College of Law.

how to best address these concerns without stifling tech companies' ability to innovate and use data to provide greater services to consumers.[7]

In the United States, the most recent attempt to balance business interests and consumer concerns has come from California, in the form of the California Consumer Protection Act (the "CCPA," or the "Act"), which went into effect January 1, 2020.[8] The Act has created a seemingly robust set of rights for consumers to know what information businesses have about them, what is being done with that information, and how they may request to delete such information.[9] However, the CCPA has also left businesses confounded on how to properly comply with the Act because of its amorphous reasonableness standard.[10] As the Act continues to proliferate into the ordinary course of business, courts should adopt a clear reasonableness standard that aids administration and business planning.

Part II of this Note will discuss the motivation for enacting the CCPA and who the Act applies to. Part III of this Note will discuss the rights and obligations provided by the CCPA and address compliance concerns for businesses. Part IV of this Note will argue that courts should resolve impending disputes by implementing a reasonableness standard informed by California Department of Justice guidelines and industry frameworks. Part V will conclude.

II. BACKGROUND

The CCPA seeks to address a growing fear over how companies may manipulate, monetize, and further utilize consumer personal data.[11] Personal information that is collected allows businesses to make sophisticated inferences about who consumers are, what they want, and what they are likely to do.[12] This information helps determine what consumers are doing, but also helps in influencing consumer behavior for future transactions.[13] These potential uses raise many concerns elaborated on below.

A. Consumer Concerns

On one hand, consumers are afraid of their behavior becoming a commodity to be traded, their choices being disempowered, and their personal autonomy being violated.[14] On the other, consumers also want the convenience and utility benefits produced by big data collection.[15] The CCPA has attempted to mitigate these conflicting interests and empower

---

7. Stewart Wolpin, *CES Panelists: Federal Law Needed to Balance Privacy and Innovation*, TWICE (Jan. 9, 2020), https://www.twice.com/industry/ces/ces-2020-panelists-federal-law-needed-to-balance-privacy-innovation.

8. Richi Jennings, *CCPA, California's GDPR, confuses and confounds*, TECHBEACON (Jan. 2, 2020), https://techbeacon.com/security/ccpa-californias-gdpr-confuses-confounds.

9. *See* Sara Morrison, *California's new privacy law, explained*, VOX (Dec. 30, 2019, 6:50 PM), https://www.vox.com/recode/2019/12/30/21030754/ccpa-2020-california-privacy-law-rights-explained.

10. *See* Jennings, *supra* note 8.

11. *See* Jacob Silverman, *How Tech Companies Manipulate Our Personal Data*, N.Y. TIMES (Jan. 18, 2019), https://www.nytimes.com/2019/01/18/books/review/shoshana-zuboff-age-of-surveillance-capitalism.html.

12. *See id.*

13. *Id.*

14. *Id.*

15. Larry Alton, *5 Ways Big Data Benefits Consumers*, CUSTOMERZONE360 (June 26, 2015), https://www.customerzone360.com/topics/customer/articles/405714-5-ways-big-data-benefits-consumers.htm#.

consumers by providing ways to find out what companies know about them and decide for themselves what is done with that information.[16]

The need for new legislation in this area is largely a result of the influx of massive amounts of consumer data and security breaches related to that data.[17] More than 90% of the world's collected data appeared in just the past two years and most of this information has been collected without consumers' explicit permission by such means as wearable technology and online forms.[18] This collection is exacerbated because modern consumer "contracts" have largely been delivered through unintelligible boilerplate where consumers are rarely, if ever, reading privacy policies.[19] Accordingly, the collection, storage and sale of personal information has been imposed on consumers without any real sense of cooperative communication or mutual understanding.[20] As a result, consumers are concerned they are giving up rights they would not have relinquished if given notice—an issue addressed by the CCPA through mandatory disclosure provisions.[21] Through its opt-out and deletion request provisions, the CCPA has also provided ways for consumers to retake control of personal information that was unknowingly relinquished.[22]

B. Who is subject to the CCPA?

The CCPA imposes rules regarding how certain for-profit companies doing business in California collect, store, and use California consumers' personal information.[23] Under the Act, companies subject to its provisions include for-profit entities that do business in California, collect consumers' personal information, and determine how that information is used.[24] Businesses must also meet at least one of the following thresholds: (1) an annual gross revenue in excess of twenty-five million dollars; (2) alone or in combination with others buy, sell, or otherwise use for a business purpose the personal information of 50,000 or more consumers, households, or devices; or (3) derive fifty percent or more of its annual revenue from selling consumers' personal information.[25]

Such businesses include Facebook, the social media giant with a 2019 gross revenue of 70.7 billion that collects a wealth of California residents' personal information through its popular social media applications.[26] Some commentators have suggested that large

---

16. *See* Michael Fertik, *CCPA Is A Win For Consumers, But Businesses Must Now Step Up On CX*, FORBES (Jan. 27, 2020, 5:40 PM) https://www.forbes.com/sites/michaelfertik/2020/01/27/ccpa-is-a-win-for-consumers-but-businesses-must-now-step-up-on-cx/#4bfda6e65574.

17. *See id.*

18. *See id.*

19. *See generally* Robin Bradley Kar & Margaret Jane Radin, *Pseudo-Contract and Shared Meaning Analysis*, 132 HARV. L. REV. 1135 (2019).

20. *See id.*

21. *See* CCPA § 1798.130(a)(5).

22. *See* CCPA § 1798.120(a)-(c).

23. Ian Mclin, *Sweeping New California Data Privacy Law Takes Effect*, JD SUPRA (Mar. 4, 2020), https://www.jdsupra.com/legalnews/sweeping-new-california-data-privacy-45158/

24. *See* California Consumer Protection Act ("CCPA") §1798.140(g) (2018).

25. *Id.*

26. *See Facebook's Annual Revenue from 2009 to 2019*, STATISTA *https*://www.statista.com/statistics/268604/annual-revenue-of-facebook/; *See also* Queenie Wong, *CCPA: What California's New Privacy Law Means for Facebook, Twitter Users*, CNET (Jan. 3, 2020), https://www.cnet.com/news/ccpa-what-californias-new-privacy-law-means-for-facebook-twitter-users/

companies such as Facebook will not be impacted by the Act because of their first-party relationships with consumers combined with the fact they do not "sell" personal information in the traditional sense.[27] However, the CCPA defines the "sale" of personal information broadly, including data transfers that result in the company receiving any monetary or valuable consideration.[28] The CCPA also reaches companies like Facebook by directly addressing large-scale political ad targeting disclosure and personal information use such as the Cambridge Analytica scandal.[29]

Smaller actors in the online advertising world and their business practices are likely to be affected by the Act as well.[30] For example, Drawbridge is a company that uses data such as IP addresses and GPS-derived locations to find out multiple devices a particular consumer owns to serve advertisements across each device.[31] This "cross-device targeting and attribution" practice is a common practice of modern digital advertising that falls subject to the Act's prohibitions.[32] In addition, "data onboarding" practices by companies such as LiveRamp will also be subject to the CCPA.[33] This practice joins offline purchases with online advertising by taking personal data such as names, addresses, and phone numbers from in-store retail purchases and combining that information with data from publishers such as email newsletters and dating sites to identify consumers and market other products directly.[34] With its breadth of prohibitions and provisions, the CCPA will have significant impact on behemoths like Facebook and Amazon, as well as mid-sized companies such as Drawbridge and LiveRamp.

The CCPA's definition of consumers under the Act is much more straightforward: a consumer is a natural person who is a California resident, as defined by the California Code of Regulations.[35] This includes (1) every individual who is in the State for other than a temporary or transitory purpose and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose.[36] Any of these Californians qualify for the protections of the CCPA and its private right of action, but will have to wait until July 1, 2020 for courts to evaluate whether the practices of a specific company are consistent with this new legislation.[37] When that time comes, courts will need to develop an equitable reasonableness standard.

---

27. *See* Antonio Garcia Martinez, *Why California's Privacy Law Won't Hurt Facebook or Google*, WIRED (Aug. 31, 2018), https://www.wired.com/story/why-californias-privacy-law-wont-hurt-facebook-or-google/

28. *See* Scott Ikeda, *Facebook Refuses to Change Web Tracking Practices, Believes That CCPA Does Not Apply to Them*, CPO Magazine (Jan. 6, 2020), https://www.cpomagazine.com/data-protection/facebook-refuses-to-change-web-tracking-practices-believes-that-ccpa-does-not-apply-to-them/

29. *See* Alvin Chang, *The Facebook and Cambridge Analytica Scandal, Explained With a Simple* Diagram, VOX (May 2, 2018), https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

30. *See* Martinez, *supra* note 27.

31. *See id.*

32. *Id.*

33. *Id.*

34. *Id.*

35. CCPA § 1798.140(g)

36. 18 CCR § 17014 (1954) ("Who are Residents and Nonresidents").

37. Gary Guthrie, *New California Privacy Law May Require Facebook to Completely Change How It Does Business*, CONSUMERAFFAIRS (Feb. 19, 2020), https://www.consumeraffairs.com/news/new-california-privacy-law-may-require-facebook-to-completely-change-how-it-does-business-021920.html

III. ANALYSIS

The enactment of the CCPA has sparked the need for new procedures for businesses to participate in the California market. Such procedures include updating privacy policies, implementing security protections, and facilitating consumer requests.[38] Additionally, because California is the world's fifth largest economy, the many companies that desire to participate in that market will make the effect of the CCPA exceedingly unlikely to remain localized.[39] Accordingly, the CCPA itself affects out-of-state companies,[40] and similar regulations are likely to be implemented in other states as well.[41]

The expense of updating policies and procedures to comply with the CCPA has been estimated to cost businesses a total of $55 billion in initial charges; a cost that will likely be passed on, even if indirectly, to consumers themselves.[42] This cost ranges from approximately $50,000 for companies with fewer than twenty employees to $2 Million for companies with greater than 500 employees.[43] Much of these charges stem from technology and operations costs associated with implementing compliance procedures as well as more detailed training and recordkeeping requirements.[44]

A motivating factor for businesses to comply with the CCPA is the private right of action granted by the Act that creates significant fines (between $100 and $750 per consumer, per incident) for failure to implement *reasonable* security measures.[45] For example, a data breach affecting one million California consumers may result in statutory damages between $100 million and $750 million; these potential damages dwarf almost every previous large data breach settlement in the United States.[46] Therefore, even though the cost of compliance is high, the risk of massive penalties for security breaches is even greater. Companies will be motivated and well-advised to implement those security measures that would be deemed reasonable should a dispute arise. To provide clarity, either the California courts or amendments to the CCPA regulations should adopt a clear and equitable reasonableness standard as it relates to security procedures.

---

38. *See* Anna Attkisson, *How California's Consumer Privacy Act Will Affect Your Business*, BUSINESS NEWS DAILY (Dec. 31, 2019), https://www.businessnewsdaily.com/10960-ccpa-small-business-impact.html

39. *See* Fertik, *supra* note 16.

40. Andrew R. Lee, *How the California Consumer Privacy Act Could Impact Your Business*, THE NAT'L LAW REV. (Nov. 20, 2019), https://www.natlawreview.com/article/how-california-consumer-privacy-act-could-impact-your-business.

41. Jedidiah Bracy, *With the CCPA now in effect, will other states follow?*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 2, 2020), https://iapp.org/news/a/with-the-ccpa-now-in-effect-will-other-states-follow/.

42. *See id.*

43. Aly McDevitt, *CCPA Compliance Costs Projected to Reach $55B*, COMPLIANCE WEEK (Oct. 8, 2019 11:40 AM), https://www.complianceweek.com/data-privacy/ccpa-compliance-costs-projected-to-reach-55b/27847.article

44. *See id.*

45. *See* CCPA § 1798.150(a)(1).

46. *See* Jaime B. Petenko, *The California Consumer Protection Act and 'Reasonable Security': A Game Changer*, MCDERMOTT WILL & EMERY (Jan. 9, 2020), https://www.mwe.com/insights/the-california-consumer-privacy-act-and-reasonable-security-a-game-changer/.

A. What is Personal Information?

With the enactment of the CCPA, Californians are given an expanded set of rights regarding the collection, sale, and storage of their personal information.[47] Under the Act, personal information includes any information that either directly or indirectly identifies, relates to, or describes a particular consumer or household.[48] The CCPA provides an extensive, but non-exhaustive, list of information capable of identifying a consumer or household.[49] This includes varying types of personal information such as biometric data and contact information, as well as electronic network activity information such as browsing history and geolocation data.[50]

The CCPA further expands the scope of what information is covered to include any information that is reasonably capable of being associated with or could reasonably be linked to a particular consumer or household.[51] What is reasonably capable of being associated with a particular consumer or household is in some circumstances ambiguous. Part of this ambiguity is because the purpose for which information is used could inadvertently make something reasonably capable of identifying a consumer. For example, a system of satellites determining the location of city buses set up by a transportation agency could make it possible to track those buses in real time and offer a better service with more accurate bus schedules.[52] This data would relate to the buses, not the drivers, however, the system could also be monitoring if the bus driver is respecting speed limits and following appropriate itineraries, and therefore may be capable of being associated with the individual driver.[53]

There is room for debate as to (1) what constitutes personal information; (2) what kind of nexus must exist between the information and the consumer or household; and (3) whether an individual consumer or household to which that information is associated with can be identified under the CCPA.[54] Future disputes easily arising over whether information a consumer is requesting should be disclosed or deleted satisfies the three elements above and can fall under one of the categories of information that is excluded from the scope of the Act: (1) de-identified data; (2) aggregated consumer information; or (3) certain types of publicly available information.[55] Businesses are likely to assert that the information they have collected or sold is not *reasonably* capable of association because burdensome steps would be needed to make an association with an individual or household.[56]

---

47. *See* California Consumer Protection Act §§ 1798.100, 1798.105, 1798.110, 1798.115
48. CCPA § 1798.140(o)(1).
49. *See id.*
50. *See id.*
51. *See id.*
52. Lydia de la Torre, *What is "Personal Information" Under CCPA?*, California Lawyers Association ((https://calawyers.org/antitrust-ucl-and-privacy/what-is-personal-information-under-the-california-consumer-privacy-act/
53. *Id.*
54. *See id.*
55. *See id.*
56. Mark Smith, *ANALYSIS: Five Wins for Business in CCPA Amendments?*, BLOOMBERG LAW (Sep. 23, 2019, 5:46 AM), https://www.bloomberglaw.com/product/privacy/document/X70ISN8S000000

B. Consumer Rights, Business Obligations, and Exceptions Under the CCPA

The principal rights consumers acquire in relation to their personal information include the right to: (1) know what personal information is being collected about them and request that information be deleted; (2) know whether their personal information is sold or disclosed and to what types of third parties; (3) opt out of having their personal information sold to or shared with third parties; (4) access a copy of their personal information; and (5) equal service and price, even when they exercise any of the aforementioned rights.[57] Businesses are required to comply with the Act through obligations that correspond to these consumer rights.[58] Among other requirements, businesses are primarily required to (1) make required disclosures; (2) respond to verified consumer rights requests; (3) respond to sales or disclosure opt-out requests; (4) refrain from discrimination; and (5) implement reasonable security practices and procedures.[59] While the Act imposes these obligations on businesses, it also provides for circumstances under which those businesses are not required to comply with consumer requests.[60] Information that is required for businesses to (1) uphold legal obligations; (2) maintain security and existing functionality; (3) protect free speech; (4) conduct research; and (5) allow for internal, expected, and lawful uses, are excluded from the scope of business obligations under the CCPA.[61]

While some businesses have made deletion requests and opt-out forms user-friendly using reasonably conspicuous forms,[62] other businesses have made the opt-out and deletion request mechanisms so confusing or difficult to navigate that consumers are unable to achieve what the CCPA is set out to accomplish.[63] For example, some companies are using what are called "dark patterns," a type of user interface design that tries to trick users into making certain choices, often against their best interests.[64] Dark pattern design can be used in a number of ways,[65] but the key element is the use of manipulative timing to exploit content-overloaded consumers into skimming material they are presented with,[66] e.g. using brightly colored "agree and continue" or "Okay, looks great!" buttons, while opt-out buttons and privacy policies often comprise greyscale text on a grey background.[67]

Exceptions and exemptions help businesses balance their interests against consumers' privacy concerns,[68] but could also contribute to legal disputes over many issues, including how information is classified.[69] While these classifications are not always abundantly clear, it seems compliance with certain CCPA provisions may yet have unforeseen implications for

57. *See* Morrison, *supra* note 9.
58. *See id.*; *See also* CCPA §§ 1798.125, 1798.130, 1798.135, 1798.150.
59. *See* Morrison, *supra* note 9; *See also* CCPA §§1798.125, 1798.130, 1798.135, 1798.150. (business obligations?)
60. *See* CCPA § 1798.105(d)(1)-(9).
61. *See id.*; *See also* SIXFIFTY, *CCPA Deletion Exemptions*, https://www.sixfifty.com/ccpa-exemptions/.
62. Such as those created by OneTrust, https://www.onetrust.com/.
63. *See* Zack Whittaker, *California's new privacy law is off to a rocky start*, TECHCRUNCH (Feb. 8, 2020, 11:00 AM), https://techcrunch.com/2020/02/08/ccpa-privacy-law-rocky-start/
64. *See id.*
65. Natasha Lomas, *WTF is dark pattern design?*, TECHCRUNCH (July 1, 2018, 12:52 PM), https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/.
66. *See id.*
67. *Id.*
68. *See* SIXFIFTY, *supra* note 61.
69. *See* de la Torre, *supra* note 52.

anticipated or pending litigation, e.g. a legal obligation (such as discovery requests) of a business could require denial of an otherwise compulsory deletion of consumer information.[70] Further, while companies intentionally attempting to influence consumer "choice" by using methods such as dark pattern design raises many concerns, amorphous "reasonableness" standards applied to personal information and security procedures under the CCPA[71] do not help companies respond in a consistently meaningful way on the whole.

Numerous disputes are likely to arise from the complex interaction of these new consumer rights, business obligations, and exceptions, e.g. how information is classified and consequently what must be disclosed or deleted and by what procedure;[72] what constitutes a 'sale' of personal information;[73] and even constitutional issues regarding the regulation of interstate commerce.[74] However, because the private right of action in the event of a security breach is the most obvious risk for private litigation[75], this Note focuses on what should amount to *reasonable* security practices and procedures.

C. Reasonable Security and the Private Right of Action

The private right of action under the CCPA includes the availability of statutory damages if a consumer's "nonencrypted and nonredacted personal information" is "subject to unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain *reasonable* security procedures."[76] Thus, plaintiffs may have a cause of action against companies who fall victim to data breaches under either a theory of a statutory violation or negligence per se.[77]

However, the reasonableness standard as it relates to CCPA compliance is as of yet ill-defined, and companies have varying interpretations of what compliance actually requires.[78] Some businesses have begun to implement the 'core considerations' of the CCPA on a global level.[79] These efforts aid compliance while signaling to all consumers that their privacy is valued by the company.[80]

---

70. *See* Allison Douglis & David Saunders, *How the CCPA impacts civil litigation*, INT'L ASS'N OF PRIVACY PROF'LS (Jan. 28, 2020), https://iapp.org/news/a/how-the-ccpa-impacts-civil-litigation/.

71. *See* Smith, *supra* note 56.

72. *See* de la Torre, *supra* note 52.

73. *See* Tim Peterson, *'We're not going to play around': Ad industry grapples with California's ambiguous privacy law*, DIGIDAY (Dec. 19, 2019), https://digiday.com/marketing/not-going-play-around-ad-industry-grapples-californias-ambiguous-privacy-law/.

74. Amy Miller, *Definition of 'sale' looms as enforcement issue for landmark California privacy law*, MLEX MARKET INSIGHT (Dec. 30, 2019), https://mlexmarketinsight.com/insights-center/editors-picks/area-of-expertise/data-privacy-and-security/definition-of-sale-looms-as-enforcement-issue-for-landmark-california-privacy-law.

75. Jessica B. Lee, Wook Hwang, Susan E. Israel, & William Grosswendt, *CCPA: A Spotlight on the Litigation Risks*, LOEB & LOEB LLP (Jan. 2, 2020), https://www.loeb.com/en/insights/publications/2020/01/ccpa-a-spotlight-on-the-litigation-risks

76. *See* Kevin Benedicto, W. Reece Hirsch, Mark Krotoski, Carla Oakley, & Gregory Parks, *Preparing for the CCPA Private Right of Action For Certain Security Incidents – Morgan Lewis Practical Advice on Privacy: Guide to the CCPA*, JD SUPRA (Jan. 6, 2020), https://www.jdsupra.com/legalnews/preparing-for-the-ccpa-private-right-of-12835/.

77. California Practice Guide: Privacy Law Constitutional/Common Law Privacy chapter 2(5)(a)(1)(a)-(b) "private right of action and other theories"; "meaning of reasonable security procedures"

78. *See id.*

79. *See* Mark Smith, *ANALYSIS: Microsoft to Extend CCPA Nationwide; Should You?*, BLOOMBERG LAW (NOV. 18, 2019, 1:00 PM), https://www.bloomberglaw.com/product/privacy/document/XKNVVD0000000

80. *See id.*

The lack of guidance as to the proper reasonableness standard set out in the CCPA will provide a breeding ground for litigation over the applicability of provisions of the Act as discussed above.[81] In response, courts should adopt a reasonableness standard informed by trade usage and recent trends in privacy law.

IV. RECOMMENDATIONS

Given that enforcement of the CCPA will begin in July 2020,[82] companies have little time to comply with the Act's regulations. Inevitably, the ambiguity within the Act as to what constitutes reasonable security of consumer information will lead to disputes and courts will have to develop a consistent standard of reasonableness for adjudicating CCPA complaints. While the CCPA does not define "reasonable security," the California Civil Code does provide some guidance,[83] noting that security procedures and practices should be appropriate to the nature of the information.[84] This suggests that what may be appropriate security for one type of information may not be appropriate for another. However, no California statute has yet defined how to determine what would be sufficiently appropriate in any given situation.[85] Drawing this line in data breach cases is likely to be a fact-specific inquiry, and some courts have noted that because of complex technical issues, expert testimony may be required.[86]

Nevertheless, reasonableness should be determined as a matter of law if a company makes a showing of (1) compliance with the twenty data security controls published by the Center for Internet Security (CIS); and (2) compliance with the National Institute of Standards and Technology cybersecurity framework ("NIS Framework"). This test would allow courts to at least determine what is clearly *not* reasonable and what clearly *is* reasonable.

A. Center for Internet Security Controls

The California Department of Justice ("DOJ") released a data breach report in 2016 that identified the "the minimum level of information security that all organizations that collect or maintain personal information should meet."[87] This report included twenty data security controls published by the Center for Internet Security (CIS).[88]

The report included basic controls, such as inventory and control of hardware assets and software assets; continuous vulnerability management; controlled use of administrative privileges; and maintenance, monitoring and analysis of audit logs.[89] Further, they include

---

81. *See* Smith, *supra* note 56.

82. *See* CCPA § 1798.185(c).

83. *See* Petenko, *supra* note 46

84. California Civil Code § 1798.81.5(c) "Security procedures and practices with respect to personal information about California residents" (2020)

85 *See Supra* note 77.

86. *See In re Anthem Litig. (ND CA 2018) 327 FRD 299, 315; See also In re TD Ameritrade Account Holder Litig. (ND CA 2011) WL 4079226, *5 (citing "complex technical issues" requiring ""substantial expert testimony" as one justification for approving class action settlement in data breach cases.).*

87. *See* supra note 46

88. *Id.*

89. *Id.*

foundational controls such as email and web browser protections; malware defenses, data recovery capabilities, controlled access based on the need to know, and account monitoring and control.[90] Lastly, organizational controls such as incident response and management and penetration tests and red team exercises were also included.[91] The DOJ noted that failure to implement all of these controls constitutes lack of reasonable security.[92] This determination was made after a DOJ review of 657 data breaches revealed that many could have been prevented or corrected more rapidly had the basic CIS security measures been implemented.[93] To the point of reasonableness, the CIS recommendations emphasizes that the benefits of implementing the controls outweigh the costs in the event of a breach. This is true even for smaller businesses since the controls are intended to be scalable to organizations of all sizes.[94]

However, this guidance from the DOJ only tells litigants that implementing these controls is necessary rather than sufficient to establish reasonable security. Accordingly, when courts are presented with disputes under the CCPA's private right of action, the CIS controls should be the first step of the court's analysis: if the company has failed to implement them, there was no reasonable security, and if the controls were implemented, the court should proceed to see what additional measures, if any, were implemented by the company.

B. Satisfactory Frameworks for Reasonableness

While the standard set forth by the CIS controls provides a minimum, many businesses should decide to implement elements from other industry recognized information security frameworks, such as the National Institute of Standards and Technology cybersecurity framework (the "NIST" framework).[95] The NIST framework, routinely updated and on its fifth revision, is a catalog of twenty security and privacy control groups and outlines controls for federal information systems and organizations.[96] These controls seek to (1) provide both public and private organizations with guidance and safeguarding measures to make information systems more resistant to cyberattacks; (2) protect the confidentiality, integrity, and availability of the organizations' information system; (3) limit the negative impact of cyber-attacks when they occur; and (4) make these information systems more survivable and resilient in general.[97]

Alternatively, other companies have been implementing security standards published by the International Organization for Standardization (the "ISO27001" framework).[98] The ISO27001 framework applies to all types of organizations and uses a risk management

---

90. *Id.*
91. *Id.*
92. *Id.*
93. CAL. ATT'Y GEN., California Data Breach Report, 32 (Feb. 2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf
94. *Id. at 31.*
95. Ronald Sarian, *What Are "Reasonable Security Procedures" Under The CA Consumer Privacy Act?*, JD SUPRA (Jan. 16, 2020), https://www.jdsupra.com/legalnews/what-are-reasonable-security-procedures-42839/
96. Katharina Gerberding, *NIST, CIS/SANS 20, ISO 27001 – Simplifying Security Control Assessments*, HITACHI SYSTEMS SECURITY (Sept. 5, 2017), https://www.hitachi-systems-security.com/blog/nist-cissans-20-iso-27001-simplifying-security-control-assessments/
97. *Id.*
98. *Id.*

framework to identify, analyze, and address an organization's information risks to protect against cyberthreats and data breaches.[99]

While the ISO27001 framework is less technical and focuses on risks for organizations of all shapes and sizes,[100] the NIST framework is more security control driven with a wide variety of groups to facilitate best practices related to federal information systems.[101] Both are useful for data security and risk management and both have the added benefit of being updated over time.[102]

Further, these standards are considered to be the gold standards of security[103] and if a company fulfills the requirements for their certification, courts should deem the company as having implemented reasonable security procedures and practices as a matter of law. The NIST and ISO27001 offer much more comprehensive approaches to data security than does the baseline CIS controls.[104] However, these security measures are costly, time-consuming to implement, and may be more than what is needed for smaller companies[105] whereas larger companies are more likely to have the ability to assume the cost of implementing more stringent controls. Nonetheless, implementing either of these standards combined with compliance with the CIS controls should be seen by courts as an outer limit that evidences reasonable security procedures and practices and adjudicate middling attempts on a case-by-case basis with assistance from expert witnesses and consideration of company size.

C. Other Privacy Statutes

Alternatively, courts could look to compliance with other privacy regimes to determine reasonableness. Many companies have implemented elements of reasonable security through their efforts to comply with other information security requirements such as the EU's General Data Protection Regulation ("GDPR").[106] Courts adjudicating reasonable security under the CCPA could take guidance from the GDPR because it is in some ways a more stringent standard for consumer privacy than the CCPA,[107] and decide that if a company has complied with the GDPR, their security procedures and practices are reasonable for purposes of the CCPA as well.

However, while these compliance efforts can be helpful and indeed show good-faith attempts at protecting consumer information, compliance with another continent's set of security requirements is unnecessary to show compliance with the CCPA.[108] For example, provisions of the CCPA specifically exclude several categories of personal information from its scope (e.g. publicly available information), while the GDPR does not exclude specific

---

99. *Id.*

100. *NIST vs. ISO: What's the Difference?*, RECIPROCITY, https://reciprocitylabs.com/resources/nist-vs-iso-whats-the-difference/.

101. *Id.*

102. *Id.*

103. *See* Sarian, *supra* note 95; *See also* Gerberding, *supra* note 96.

104. *See* Cal. Att'y Gen., *supra* note 93.

105. *See* Sarian, *supra* note 95.

106. *See id.*

107. *See* Geoffroy De Cooman, *GDPR and CCPA compliance: The 5 differences you should know*, PROXYCLICK (Oct. 7, 2019), https://www.proxyclick.com/blog/gdpr-and-ccpa-compliance-5-differences

108. *See id.*

categories of personal data from its scope of application.[109] Additionally, the CCPA also excludes several specific processing activities from the definition of "selling," for example, where a business shares personal information with a service provider that is necessary for a "business purpose," as defined in the CCPA.[110] Conversely, the GDPR does not exclude this type of processing activity.[111] As a result of these dissimilarities there could be circumstances where a company discloses personal information to a third party for a business purpose that would be in compliance with the CCPA, yet would create security concerns under the GDPR. Further, the GDPR provides for certain legal grounds on which a company may collect personal information, while the CCPA does not provide for such limitations as an initial matter and instead functions as a quasi-consumer consent mechanism.[112] Accordingly, applying GDPR compliance in a wholesale manner may be too burdensome in certain circumstances because the two statutes cover different types of information and different processing methods of that information.

In resolving forthcoming disputes, courts should apply a reasonableness standard that sets the minimum standard set forth by the CIS controls[113] as a benchmark and a further showing of NIST framework compliance[114] or ISO27001 certification[115] to constitute reasonable security as a matter of law. Compliance with GDPR provisions could be helpful in adjudicating a company's security measures but will not be dispositive in many cases because of the substantive differences in breadth and scope between the two regimes.

V. CONCLUSION

Legislation such as the CCPA is a much-needed effort to address issues of consumer privacy while balancing business interests such as innovation. However, the rush to its enactment[116] has created ambiguity and confusion that will lead to legal disputes that risk heavy penalties for businesses involved.[117] To aid in resolving forthcoming disputes, courts should adopt a reasonableness standard that uses the CIS controls as a benchmark and compliance with the NIST or ISO frameworks as clearly evidencing reasonable security procedures and practices. While this field is ever-changing and updates may be required as future frameworks are developed, this test is easily administered and would provide businesses with much-needed clarity for compliance.

---

109. *See Comparing privacy laws: GDPR v. CCPA* at 11, DATAGUIDANCE & FUTURE OF PRIVACY FORUM (Last accessed May 28, 2020) https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf (accessed through https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/)

110. *See id.* at 12.

111. *See id.*

112. *See id.* at 23.

113. *See* Petenko, *supra* note 46.

114. *See id.*

115. *See id.*

116. *See* Jennings, *supra* note 5.

117. *See* Benedicto, et. al, *supra* note 16.