

Summer 2020

American Privacy Law at the Dawn of a New Decade (and the CCPA and COVID-19): Overview and Practitioner Critique

Kimberly Dempsey Booher

Martin B. Robins

Follow this and additional works at: <https://scholarship.law.marquette.edu/iplr>



Part of the [Intellectual Property Law Commons](#), [International Law Commons](#), [Privacy Law Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Kimberly D. Booher & Martin B. Robins, *American Privacy Law at the Dawn of a New Decade (and the CCPA and COVID-19): Overview and Practitioner Critique*, 24 Marq. Intellectual Property L. Rev. 169 (2020).

This Article is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. It has been accepted for inclusion in Marquette Intellectual Property Law Review by an authorized editor of Marquette Law Scholarly Commons. For more information, please contact megan.obrien@marquette.edu.

AMERICAN PRIVACY LAW AT THE DAWN OF A NEW DECADE (AND THE CCPA AND COVID- 19): OVERVIEW AND PRACTITIONER CRITIQUE

Note: This article was finalized by the authors and editors on November 10, 2020 and does not discuss any developments which may have occurred thereafter. In light of the extraordinarily rapid evolution of law and practice in this area, readers are urged to take into account the possibility of intervening developments, including potential action regarding legislation pending at that date.

KIMBERLY DEMPSEY BOOHER

MARTIN B. ROBINS*

I. INTRODUCTION: WHAT DO WE MEAN BY PRIVACY?	170
II. SOURCES AND SUBJECTS OF PRIVACY LAW AND GUIDANCE	174
III. EUROPEAN UNION GENERAL DATA PROTECTION REGULATION.....	177
IV. BREACH NOTIFICATION LAWS	179
V. AFFIRMATIVE SECURITY AND OTHER OBLIGATIONS	180
VI. FTC RULES AND ADMONITIONS—DISCLOSURE—BASED AND OTHER... 183	
VII. CHILDREN’S ONLINE PRIVACY PROTECTION ACT (“COPPA”)	186
VIII. CALIFORNIA CONSUMER PRIVACY ACT (“CCPA”).....	189
IX. ROLE OF PRIVACY POLICIES	193
X. CRITIQUE AND RECOMMENDATIONS: GENERAL AND RESPONSIVE TO COVID-19 DEVELOPMENTS.....	195

* Both authors are partners practicing in the Privacy and Corporate Practice Groups at the international law firm of FisherBroyles, LLP, Ms. Booher in the Palo Alto, California office and Mr. Robins in the Chicago, Illinois office. Both hold J.D. degrees (cum laude) from Harvard Law School, 1998 for Ms. Booher and 1980 for Mr. Robins. Ms. Booher holds a B.A. degree (summa cum laude) from Boston University while Mr. Robins holds a B.S. degree (summa cum laude) from the Wharton School of the University of Pennsylvania. Feedback is encouraged: the authors may be reached at kimberly.booyer@fisherbroyles.com and martin.robins@fisherbroyles.com.

The views expressed herein are solely those of the authors and not those of FisherBroyles, LLP.

A. Breach Notification Statutes.....	195
B. State Substantive Regulation	197
C. Informal FTC Regulation	197
D. Children’s Online Privacy Protection Act.....	198
E. Information Collection and Usage; Present law: Opt-in; Opt-out	199
XI. COVID-19 AND PRIVACY.....	202
A. Alternative Technologies.....	203
B. Voluntary vs Mandatory: Legal and Health Ramifications	203
C. Non-US Mandatory Approach.....	206
D. Need for Unified Approach	207
XII. CONCLUSION	208
APPENDIX	209

I. INTRODUCTION: WHAT DO WE MEAN BY PRIVACY?

The topic of privacy comes up very frequently today. Apart from the extensive discussion in technology and academic circles, within the political arena this is apparently the closest thing to a bipartisan concern,¹ and the popular press and business-oriented legal environment all treat the subject as a high priority. COVID-19 and a fervent desire by all to use technology to reduce the likelihood of its recurrence are justifiably major factors in current discussions, but equally justifiable concerns about the impact of such technology on Americans’ privacy also demand a good deal of attention on privacy law as it stands and as some may seek to change it. For example, as this article was being finalized, the Wall Street Journal reported that in an effort to expedite employees return to work following virus-related lockdowns, “United Health and Microsoft Corp. jointly developed an app that checks worker symptoms and gives a go-ahead to report to work.”²

1. For example, when commenting on pending legislation, Republican Sen. Josh Hawley stated: “I hope once more that the perfect won’t be the enemy of the good. . . . I hope that in the next year — still in this Congress — that [the] Commerce [Committee] and others will say, ‘You know what? We can get some things done.’” Jessica Smith, *Will 2020 be the year of a federal privacy law?*, YAHOO FIN., (Dec. 23, 2019), <https://finance.yahoo.com/news/will-2020-be-the-year-of-a-federal-data-privacy-law-185226703.html>. Of course, this was the view prior to the COVID-19 outbreak.

2. Sarah Krouse, *Bosses Begin Testing Workers for COVID-19*, WALL ST. J., (May 25, 2020), https://www.wsj.com/articles/covid-19-tests-come-to-work-11590399001?mod=hp_lead_pos3. In the same article, a human resources executive stated that ‘health questions once deemed too intrusive are now necessary for workplace safety.’ This may be medically correct but ignores the fact that applicable privacy laws did not change during the pandemic. Several bills are pending in Congress to regulate the use of such apps. For example, Sens. Cantwell, Klobuchar, and Cassidy introduced the Exposure Notification Act. See note 165 and accompanying discussion.

Yet, there is a good deal of disagreement as to what ‘privacy’ actually entails and why it should be prioritized. This article intends to explain the different objectives and authorities incorporated into this area of law and provide the authors’ own views, as experienced practitioners advising technologically-oriented businesses, of what social utility is being provided, and at what operational cost, and what should be adjusted.

A brief background to the privacy landscape in the United States starts with an illustrative juxtaposition of the US and European approaches to personal information. While the European Union’s General Data Protection Regulation (GDPR)³ is a general, comprehensive law that addresses personal information regardless of whether it is collected by a bank or a hospital, the US has, at the federal level, followed a ‘sectoral’ approach with laws that address in somewhat tangential fashion security and use of particular categories of data such as, but not limited to, health information⁴ and financial information.⁵ The US has no comprehensive federal codification of authority and, at least at this writing,⁶ no generally applicable federal statute that would cover personal information not captured or preempted by existing federal legislation.

While there are a number of definitions that exist, all of privacy law deals with ‘personal information.’ Until the passage of recent laws, including the California Consumer Privacy Act (or ‘CCPA’),⁷ the ‘standard’ definition of ‘personal information’ among the states was some variety of an individual’s first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver’s license number or state-issued ID card number, (iii) bank account number, credit card number, or debit card number combined with any security code, access code, PIN, or password needed to access an account and generally applies to computerized data that includes personal information. Such definitions have tended to be bundled with data breach notification provisions, with the result being that the definition of

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [hereinafter GDPR].

4. For example, The Health Insurance Portability and Accountability Act of 1996 (‘HIPAA’), 42 U.S.C. § 300gg; 29 U.S.C § 1181 et seq.; Pub. L. No. 104-191, 42 U.S.C § 1320d et seq.; Health Information Technology for Economic and Clinical Health Act (‘HITECH Act’), Pub. L. No. 111-5, 42 U.S.C. Sec. 200 et seq.

5. Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, Pub. L. No. 106–102, 12 U.S.C. § 1811.

6. While prospects for enactment are questionable, both Senate Republicans and Democrats have introduced separate bills loosely modeled after the GDPR. Deven McGraw, *Pending Federal Privacy Legislation: A Status Update*, MEDIUM, (July 24, 2019), <https://medium.com/@citizen/the-healthcareblog-series-the-health-data-goldilocks-dilemma-privacy-sharing-both-ce4689d3fc1f>.

7. CAL. CIV. CODE § 1798.100 (West 2020) et seq.

personal information flowed from a concern about identity theft and financial harm.

With the passage of the CCPA, the US privacy landscape has undergone a sea change. The CCPA's definition of 'personal information'⁸ is not linked to those elements that, if compromised, can cause tangible harm to the individual; instead, the CCPA's definition drills down to capture what was previously thought of as non-identifying data, such as device ID and IP address, and 'drills up' to capture an amorphous and highly changeable concept of 'household.' The CCPA provides that:

'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.⁹ Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

- (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.
- (B) Any categories of personal information described in subdivision (e) of Section 1798.80.¹⁰
- (C) Characteristics of protected classifications under California or federal law.

8. CAL. CIV. CODE § 1798.140(o)(1) (West 2020).

9. While the statute does not define this term, the text of the final regulations defines "household" as "a person or group of people who: (1) reside at the same address, (2) share a common device or the same service provided by a business, and (3) are identified by the business as sharing the same group account or unique identifier."

Cal. Code Regs. tit. 11, § 999 et seq., <https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-reg.pdf>.

10. In this section of California's Customer Records Act, "personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.¹¹

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g, 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.¹²

To be clear, this article intends to cover only US privacy law, of which there is a great deal to discuss among state laws,¹³ state and federal administrative pronouncements,¹⁴ and limited federal statutory law.¹⁵ However, as earlier suggested, the subject cannot be properly addressed without some understanding of the origins and influence of the GDPR, which is of great importance both of itself and as a template for US legislation and its interpretation.¹⁶

11. "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information. CAL. CIV. CODE § 1798.140(b) (West 2020). The breadth of the definition goes beyond the layman's idea of 'biometric' data to reach changeable characteristics and information captured in a pinpoint of time.

12. CAL. CIV. CODE § 1798.140(o)(1).

13. See, e.g., *infra* notes 52-72 and accompanying text.

14. See *infra* notes 64, 74-84 and accompanying text for discussion of guidance from Federal Trade Commission and California Attorney General.

15. And largely non-existent case law.

16. As this article went to press, California voters took action which will, presently as of January 1, 2023, result in closer alignment of the CCPA and GDPR. While the full implications are not yet known and may well be revised by intervening legislation or regulation, readers should remain apprised of potential implications. However, the CCPA differs from the GDPR in some significant ways,

II. SOURCES AND SUBJECTS OF PRIVACY LAW AND GUIDANCE

Unlike many articles, this one will not enumerate all material elements of existing statutory law. Rather, while such provisions will be summarized, the focus will be on presentation of informal but highly material authority which may be under the radar of more traditional discussions, as well as a discussion of whether the entire regimen provides substantial social value in itself and relative to the burdens imposed on private activity.

In the authors' experience, the term *privacy* is frequently employed to encompass one or more of the following, all of which involve a separate set of considerations and concerns:

- protection of consumers from financial crimes associated with wrongful access to their identity and online credentials through both requirement of prompt notice of data breaches¹⁷ and substantive regulation of steps to prevent them,¹⁸ as well as sporadic consideration of class action litigation pertaining to non-compliance with such legislation;¹⁹
- protection of individuals from government 'spying' on their online activities or other intrusions upon their freedom, stemming from the revelations by Edward Snowden regarding such activity by the US National Security Agency (NSA);²⁰

particularly with regard to the scope of application; the nature and extent of collection limitations; and rules concerning accountability. Regarding the latter for example, the GDPR provides for obligations in relation to the appointment of Data Protection Officers, the maintenance of a register of processing activities, and the need for Data Protection Impact Assessments in specified circumstances. Conversely, the CCPA does not specifically focus on accountability-related obligations, even though such provisions exist, such as the obligation for companies to train their staff that deal with requests from consumers. It is also noteworthy that the core legal framework of the CCPA is quite different from the GDPR. A fundamental principle of the GDPR is the requirement to have a "legal basis" for all processing of personal data. That is not the case for the CCPA. Marini et al., *Comparing Privacy Laws: GDPR v. CCPA*, FUTURE OF PRIV. F., <https://iapp.org/resources/article/comparing-privacy-laws-gdpr-v-ccpa/>, (last visited Sept. 12, 2020).

17. See *infra* notes 52-57.

18. Such as the Mass. and Fla. statutes discussed, *infra* notes 61-63.

19. *E.g.*, *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, (7th Cir. 2018); *Collins v. Athens Orthopedic Clinic, P.A.*, 307 Ga. 555 (2019). Both cases preliminarily allowed class actions to proceed based upon a finding of shared, cognizable harm.

20. A description of the rationale for GDPR by the person who is said to have triggered the effort to enact it: "Regulating the protection of data presumes that the collection of data in the first place was proper, was appropriate, that it doesn't represent a threat or a danger, that it's ok to spy on everyone all the time whether they are your customers or your citizens—so long as it never leaks, so long as only you are in control of what it is that you've stolen from everybody."

Steve Ranger, *GDPR is missing the point, says Snowden*, ZDNET, (Nov. 4, 2019), <https://www.zdnet.com/article/gdpr-is-missing-the-point-says-edward-snowden/>.

- protection of individuals from commercial tracking and oversight of their online and physical²¹ activity, whether with respect to targeted advertising or otherwise, by those authorized to possess their information;
- protection of individuals from unknown and/or unwanted sharing of any information concerning them by those authorized to possess their information; and
- special protection of children (typically those at or under age 13²²) from any third party tracking or oversight of their online activities.

In place of federal codification of authority or generally applicable federal statute, we have the following patchwork of state and federal approaches:

- Pursuant to its contested, but ultimately recognized authority to regulate ‘unfair or deceptive trade practices’ under Section 5 of the Federal Trade Commission Act of 1914,²³ the Federal Trade Commission has provided guidance and more through a series of ‘consent orders’ with names of allegedly offending companies,²⁴ formal rule making,²⁵ formal litigation such as the *Wyndham* case²⁶ and

21. Regulation of GPS or other geo-location tracking is an example. COVID-19 has made this more than an academic issue. Privacy concerns around geo-location data were prominent in Apple’s and Google’s plan to cooperatively create a system for COVID-19 contact tracing via IOS and Android mobile devices. The plan calls for using Bluetooth signals to identify devices in proximity of the device of an infected person without identifying the precise location of the devices. *Apple and Google partner on COVID-19 contact tracing*, APPLE NEWSROOM, (April 10, 2020), <https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>.

22. 15 U.S.C. § 6501 et seq.

23. 15 U.S.C. § 45; *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). One of the authors engaged in a colloquy with former Homeland Security Secretary Michael Chertoff over the significance and sufficiency of the very broad language of Section 5 to the FTC’s efforts. Agreeing with Sec. Chertoff that the FTC’s actions are “stretching the FTC’s mission beyond recognition,” the author observed that “[t]he FTC is doing a job which no other agency is prepared to do and on balance, doing it well.” Interestingly, the author’s 2012 observation that “there is no federal or meaningful state law which gives businesses guidance as to how they are to safeguard consumer information” remains largely true at this writing (notwithstanding the state laws and administrative guidance) discussed herein and lends further support to the 2012 observation that “we need an approach which is more than ‘better than nothing.’” Martin B. Robins, Letter to the Editor, *We Need a Better Approach to Protecting Electronic Data*, WALL ST. J., August 1, 2012, at A.12.

24. *E.g.*, *The TJX Companies, Inc.*, File No. 072-3055, (March 27, 2008). In a recent statement, the FTC made clear that it intended to be even more specific in its orders regarding required security practices and to require direct oversight of such practices by governing bodies and senior management. Andrew Smith, *New and improved FTC data security orders: Better guidance for companies, better protection for consumers*, FEDERAL TRADE COMMISSION, (Jan. 6, 2020), <https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance>.

25. *E.g.*, the “Red Flags Rule” found at 16 C.F.R. § 681 et seq.

26. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d at 236.

informal, but influential recommendations.²⁷ A particular focus of the FTC is the adherence of companies to the privacy policies which they post.²⁸

- Pursuant to its direct authority to enforce the Children’s Online Privacy Protection Act, the FTC promulgates rules and brings proceedings to enforce the Act where information collection from or about children has exceeded legal limits;
- As discussed *infra*, virtually every state has enacted some form of data breach notification law;
- Several, but by no means all, states have enacted substantive requirements governing companies’ obligations to secure personal information;²⁹
- Led by California through its widely publicized CCPA, several states³⁰ regulate the ability of those collecting personal information to share it with others without the informed consent of the subject,³¹ and provide such subjects with the ability to prevent such sharing.

As noted in the introduction, there are several other federal statutes which are pertinent to this area, but which are analytically distinct from those which are discussed here in detail.³²

27. *E.g.*, *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION, (October 2016), <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

28. The recently concluded Facebook episode and preceding consent decree discussed *infra* notes 76–77 and accompanying text reflect the importance of avoiding misleading disclosures in privacy policies or elsewhere.

Complaint for Civil Penalties, Injunction, and Other Relief, *U.S. v. Facebook, Inc.*, D. D.C. (2019) (No. 19-cv-2184) https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf. The authors frequently advise clients that the best way to encounter problems with the FTC is to fail to follow one’s own policy.

29. *E.g.*, *infra* notes 59-73 and accompanying text on state substantive law.

30. Nev. Leg. 220, 2019 Leg., 80th Sess. (Nev. 2019); Me. Leg. 946, 2019 Leg., 129th Sess. (Me. 2019) (An Act to Protect the Privacy of Online Customer Information currently applicable only to internet service providers, and requiring an opt-in from data subjects to allow the sharing of their information). Similar legislation is pending in several other states, most notably Washington State.

31. Through privacy policies and related disclosures, discussed *infra* notes 119–132.

32. Pursuant to its direct authority under the Telephone Consumer Protection Act, 47 U.S.C. § 227 et seq., the Federal Communications Commission enforces prohibitions of unwanted telephone (especially mobile) phone and text marketing efforts. The focus of this law is more on helping consumers to avoid annoyance and wasted phone plan minutes than privacy. At this writing, the Supreme Court of the United States agreed to entertain a constitutional challenge to the TCPA. *See Barr v. Am. Ass’n of Political Consultants*, 140 S. Ct. 2335 (2020). Pursuant to dedicated federal statutes such as the Health Information Technology for Economic and Clinical Health Act “HITECH”, 42 U.S.C. § 201 et seq., and Gramm–Leach–Bliley Act, several federal agencies, including, but not limited to the FTC, provide special oversight of personal information security in the health care and financial services fields.

III. EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

While the GDPR is, for the most part, beyond the scope of this article and the subject of a plethora of scholarship,³³ in light of the manner and extent to which it is shaping both the nature of the discussion around privacy and specific US legislation,³⁴ it is essential to understand its general confines. Critically, the law applies, without exception for *de minimus* contact, to all collection of the personal information of European Union ('EU') and United Kingdom citizens, regardless of whether the party collecting such data has a physical presence in the EU or United Kingdom.³⁵

Enacted shortly after the revelations of NSA spying on Americans and in keeping with the European emphasis on individual privacy, the law is comprised of 99 'Articles.'³⁶ The gravamen of the law consists of:

- a requirement for clear disclosure, devoid of legalese and obfuscation, of what information is being collected, with whom it is to be shared, and why it is to be shared;³⁷
- a separate requirement of affirmative opt-in for data collection and uses that are ancillary to the services requested by the data subject, such as the use of location tracking technology³⁸ (if maps or directions are not requested by the data subject);
- a requirement for the opt-in to use of 'cookies' or computer code files placed on the devices of website users by website operators;³⁹

33. *E.g.*, DAVID ZETOONY, THE EU GDPR: ANSWERS TO FREQUENTLY ASKED QUESTIONS (2018).

34. And in the opinion of the authors likely to heavily influence the construction of US legislation, at least in the first instance.

35. Subject to potential change as the Brexit is effectuated.

36. *General Data Protection Regulation*, INTERSOFT CONSULTING, <https://gdpr-info.eu/>, (last visited Sept. 12, 2020).

37. GDPR, *supra* note 3, at articles 12–13.

38. Not expressly addressed within any GDPR article, but viewed by commentators as implicit in the consent requirement of Art. 7 and discussed in Recital 25 of pending ePrivacy Regulation. David Meyer, *What the GDPR will mean for companies tracking location*, INT'L ASS'N OF PRIV. PRO., (Feb. 27, 2018), <https://iapp.org/news/a/what-the-gdpr-will-mean-for-companies-tracking-location/>. Of course, this issue has assumed even greater significance in the wake of COVID-19, as policy-makers grapple with technological measures to contain such diseases.

39. GDPR, *supra* note 3, at recital 30 and separate Cookie Directive. *Cookies, the GDPR, and the ePrivacy Directive*, PROTON TECH. AG, <https://gdpr.eu/cookies/> (last visited Sept. 12, 2020). Note that some of the related regulations have yet to be issued. Since cookies are generally dropped at the moment a user loads a website and prior to the user having an opportunity to navigate to and review a privacy policy, a consent to cookies is generally separate from the consent to other data handling practices described in the privacy policy. A 'cookie banner' usually looks something like this: "We use cookies on this website to improve functionality and performance, to analyse traffic to the website and to enable social media features. To learn more please see our Cookies Policy [hyperlinked] for details." The banner should require an action indicating consent of cookies prior to the placement on the user's

- a requirement that individuals affirmatively opt-in to the stated collections and sharing;⁴⁰
- a requirement that individuals be able to erase information pertaining to them;⁴¹
- an individual ‘right to be forgotten’ or prevent their name from coming up in internet searches;⁴²
- a requirement that collectors of data ‘map’ it to establish where it goes, whether to web hosts, analytics firms, or otherwise;⁴³
- a requirement that some data collectors formally designate and fully empower a ‘data protection officer’ with full responsibility and authority for compliance;⁴⁴
- a requirement that data breaches be reported to EU authorities within 72 hours;⁴⁵
- a requirement that anyone entrusting personal information to a third party enter into a written ‘data processing agreement’ with them providing for appropriate technical and organizational safeguards;⁴⁶
- a requirement for a formal incident response plan to deal with breaches;⁴⁷
- specific requirements around transfer of EU personal data to ‘inadequate’ countries, of which the US is one, requiring a recognized transfer mechanism, which in the US customarily involves either

device. Emerging practice is to have a menu of cookies separated by function and identified as “optional” or “necessary” with an opt-in toggle available for each. In a press release on October 1, 2019, regarding the Planet49 case, the European Union’s Court of Justice explained that pre-checked consents for cookies do not equate to affirmative opt-in consent, and that informed consent includes knowing the purpose and duration of the cookies as well as whether the information is shared with third parties. Press Release, Court of Justice of the European Union, *Storing cookies requires internet users’ active consent* (1 October 2019), <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf>.

40. GDPR, *supra* note 3, at articles 6, 7, and 13. In an early 2019 case involving Google, it was made clear that opt-in means opt-in, as Google was fined 50 million Euros for pre-checking consent boxes. Adam Satariano, *Google Is Fined \$57 Million Under Europe’s Data Privacy Law*, N.Y. TIMES, (Jan. 21, 2019), <https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html>. See also Court of Justice of the European Union, *supra* note 39.

41. GDPR, *supra* note 3, at article 17; GDPR, *supra* note 3, at recitals 65–66.

42. GDPR, *supra* note 3, at article 17(2); GDPR, *supra* note 3, at recital 66.

43. GDPR, *supra* note 3, at article 30.

44. GDPR, *supra* note 3, at article 37.

45. GDPR, *supra* note 3, at articles 33–34.

46. GDPR, *supra* note 3, at articles 24, 28, 78, and 81. In practice, DPAs often contain elaboration regarding specific measures which are utilized. Additionally, the Standard Contractual Clauses (controller-processor) require, in Appendix 2, a description of the technical and organizational security measures implemented by the data importer.

47. GDPR, *supra* note 3, at articles 32–33. Article 33’s 72-hour reporting obligation effectively requires existence of a formal response plan.

self-certification to the ‘Privacy Shield’ frameworks⁴⁸ or compliance with ‘Standard Contractual Clauses’;⁴⁹

- distinctions between those functioning as ‘controllers’ and ‘processors’;⁵⁰ and
- fines for non-compliance of up to the greater of 20 million Euros or 4% of worldwide revenue.⁵¹

The overlap between the various US laws and the more comprehensive GDPR will become apparent.

IV. BREACH NOTIFICATION LAWS

While the basic concept is largely self-explanatory insofar as it involves notice to impacted individuals, statutes vary widely with respect to matters such as:

- Numerical threshold for reporting to the state: many states apply their laws in cases involving a threshold number of impacted records (in California and Florida, for example, that is 500 records⁵²). Until very recently, Illinois did not have such a threshold, but has recently enacted one;
- Manner of reporting (to affected persons): California requires at least 10 point type and specifies headings⁵³ while Illinois is not as specific, but requires contact information for credit reporting agencies and the FTC and prohibits inclusion of the number of impacted Illinois residents;⁵⁴
- Timing and Order of Notification: the time frame within which notification must be sent to affected individuals, the time frame within

48. GDPR, *supra* note 3, at article 46. The viability of the Shield and Standard Clauses is currently the subject of EU litigation. Caitlin Fennessy, *The Privacy Shield review and its potential to impact Schrems II*, INT’L ASS’N OF PRIV. PRO., (Nov. 5, 2019), <https://iapp.org/news/a/the-privacy-shield-review-and-its-potential-to-impact-schrems-ii/>.

49. GDPR, *supra* note 3, at articles 44–47. An interesting example of the overlap between US and EU law is presented by the FTC Order in which a company was taken to task for falsely claiming that it was a participant in the authorized Privacy Shield program. Press Release, Federal Trade Commission, FTC Charges Nevada Company with Falsely Claiming Participation in the EU-U.S. Privacy Shield, (Nov. 7, 2019), <https://www.ftc.gov/news-events/press-releases/2019/11/ftc-charges-nevada-company-falsely-claiming-participation-eu-us>.

50. GDPR, *supra* note 3, at articles 24–29.

51. GDPR, *supra* note 3, at article 83.

52. CAL. CIV. CODE §§ 1798.29, 1798.80, 1798.82 (West 2016); FLA. STAT. § 501.171 (2014). Relatedly, some states, e.g., New Jersey, have a separate threshold for reporting to credit agencies. *See* N.J. STAT. ANN. § 56:8-163(f) (West 2019).

53. CAL. CIV. CODE § 1798.29.

54. 815 ILL. COMP. STAT. 530/1–530/30 (2006).

which the breach must be reported to the state, and the timing relative to each other⁵⁵ varies;

- Nature of information accessed: in California, the statute is triggered by ‘unauthorized’ acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity. Meanwhile, in Florida, the standard is essentially the same, with the critical exception that notice is not required in cases where ‘the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals.’⁵⁶ The key takeaway is that when the situation potentially arises, those responsible for compliance must look at the exact language of the statute(s) in question to determine whether they are triggered simply by access or if something more, such as evidence of fraud, is required;
- Remedial action beyond notice: for the most part, as is the case in California,⁵⁷ this involves provision of free credit monitoring for some specified interval, although not all states impose such a specific requirement.

Companies experiencing such an event have no choice but to refer to each statute in any location where it has any affected customers.

V. AFFIRMATIVE SECURITY AND OTHER OBLIGATIONS

In contrast to breach notification laws, which are not relevant unless and until a breach occurs,⁵⁸ affirmative security laws require that steps be taken to prevent such occurrence. The most notable laws are:

55. See N.J. STAT. ANN. § 56:8-163(c)(1) (West 2019) (which says notice must be provided to the state in advance of the notice to the affected individuals); LA. ADMIN. CODE tit. 16, § III-701 (2015) (requiring notice to the State of Louisiana within 10 days of distribution of notice to affected individuals).

56. FLA. STAT. § 501.171(4)(c) (2019). In California, “Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the entity. CAL. CIV. CODE § 1798.82(g). Meanwhile, the Illinois standard includes the above plus biometric information. 815 ILL. COMP. STAT. 530/5.

57. CAL. CIV. CODE § 1798.82(d)(2)(G) (West 2020).

58. Although the different statutes contain different definitions of ‘breach’, in some, mere access is sufficient to trigger the statute, while in others, there must be evidence that information was actually taken.

- The recent New York Shield law,⁵⁹ which contains some general affirmative security obligations⁶⁰ along with an enhanced version of the prior breach notification law which now covers anyone with personal information pertaining to New York residents, regardless of whether they have a place of business in New York, and adds biometric information to the definition of personal information;
- The “Florida Information Protection Act of 2014”⁶¹ which simply requires the taking of ‘reasonable’ security measures while elaborating upon the previous sparse breach notice law; and
- The more comprehensive Massachusetts version, “Standards for The Protection of Personal Information of Residents of the Commonwealth”⁶² which prescribes various technical measures such as:
 - prevention of access to sensitive information by terminated employees;
 - meaningful oversight of service providers;
 - physical access restrictions; and

59. Press Release, Governor Andrew M. Cuomo, Governor Cuomo Signs Legislation Protecting New Yorkers Against Data Security Breaches, (July 25, 2019), <https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-protecting-new-yorkers-against-data-security-breaches> (adding new Sec. 899-BB and revising Sec. 899-AA of General Business Law).

60. N.Y. GEN. BUS. LAW § 899-BB (MCKINNEY 2020). Sec. 2 of 899-BB states:

Reasonable security requirement. (a) Any person or business that owns or licenses computerized data which includes private information of a resident of New York shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information including, but not limited to, disposal of data. (b) A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either: (i) is a compliant regulated entity as defined in subdivision one of this section; or (ii) implements a data security program that includes the following: (A) reasonable administrative safeguards such as the following, in which the person or business: (1) designates one or more employees to coordinate the security program; (2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks; (4) trains and manages employees in the security program practices and procedures; (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances; and (B) reasonable technical safeguards such as the following, in which the person or business: (1) assesses risks in network and software design; (2) assesses risks in information processing, transmission and storage; (3) detects, prevents and responds to attacks or system failures; and (4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and (C) reasonable physical safeguards such as the following, in which the person or business: (1) assesses risks of information storage and disposal; (2) detects, prevents and responds to intrusions; (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

61. FLA. STAT. § 501.171.

62. 201 MASS. CODE REGS. 17.00 (2009) et seq.

- encryption of material in transit and stored on laptops and similar devices, deployment of malware protection, and meaningful user authentication protocols.⁶³

In the same vein are recommendations by the California Attorney General.⁶⁴ While these are not ‘law’ in the traditional sense of being a permissible subject of enforcement litigation, the authors view them as very useful guidance for clients⁶⁵ who desire to avoid regulatory attention and mitigate that which is unavoidable. While there is no shortage of general admonitions dictating the use of ‘good’ security practice, the California Attorney General recommendations go further insofar as they direct attention to matters such as user and administrator privileges, specific settings, and ongoing testing.

Illinois has a largely unique⁶⁶ statute governing collection and use of biometric, or physical characteristic data such as fingerprints and ‘face geometry,’⁶⁷ which requires individual consent to most uses, including those by employers. Claims under this law⁶⁸ have been determined by the Illinois Supreme Court to support class actions⁶⁹ even without specific proof of harm. Similar statutes are under consideration in other states. It seems questionable whether this statute would, absent some sort of individual notice and consent, allow

63. 201 MASS. CODE REGS. 17.03-.04 (2009).

64. Kamala Harris, *California Data Breach Report*, CAL. DEP’T JUST., (Feb. 2016), <https://oag.ca.gov/breachreport2016>.

65. *Much Needed Meat on Security Requirement Bones: Report from California’s Attorney General*, FISHERBROYLES, LLP, (Mar. 7, 2016), <https://www.fisherbroyles.com/much-needed-meat-on-security-requirement-bones-report-from-californias-attorney-general/>.

66. Washington State has very recently enacted its own version. WASH. REV. CODE. § 19.375.010 (2017) et seq.; see also Kristine Argentine, Paul Yovanic Jr., *The Growing Number of Biometric Privacy Laws and the Post-COVID Consumer Class Action Risks for Businesses*, JDSUPRA (June 9, 2020), <https://www.jdsupra.com/legalnews/the-growing-number-of-biometric-privacy-62648/>. (Illinois is apparently the only such state to allow a private right of action).

67. 740 ILL. COMP. STAT. 14 (2008) et seq. A class action lawsuit under this statute was very recently settled for a \$550 million payment. Andrew G. Simpson, *Facebook to Pay \$550 Million to Settle Biometric Privacy Violation Concerns*, INS. J., (Jan. 30, 2020), <https://www.insurancejournal.com/news/national/2020/01/30/556920.htm>; In re Facebook Biometric Information Privacy Litigation, No. 15-cv-03747-JD, 2017 U.S. Dist. LEXIS 139051, (N.D. Cal. Aug. 29, 2017).

68. In a case filed in Illinois during the writing of this article, the contemplated class plaintiff alleges that IBM violated the statute by incorporating his and other facial photos into a data base, which it made available to third parties, when it failed to obtain any consent for such usage. Class Action Complaint, Janecyk et al v. International Business Machines Corp., Ill. Cir. Ct. (January 22, 2020) (No. 2020CH00833). Following the filing of such action, IBM and Microsoft revised their internal policies to prohibit sharing of such data with law enforcement. Alex Hern, *IBM quits facial-recognition market over police racial-profiling concerns*, THE GUARDIAN, (June 9, 2020), <https://www.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns>.

69. *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (2019).

employee or patron temperature checking programs of the kind seen by many as key to mitigating coronavirus exposure. It is also possible that preemptive federal legislation will be enacted. As noted,⁷⁰ the authors advocate for the enactment of such legislation, and bills are pending.

A federal judge's skepticism regarding a substantial settlement of a class action suit under the Illinois statute, based upon his concern that it does not reflect \$100 per occurrence penalties for willful violations, portends increasing importance of the statute.⁷¹

On a related note, several other class action suits are now pending. Most notably, the American Civil Liberties Union has brought its own action under the Illinois statute against a private company, known as Clearview, on behalf of all impacted persons, specifically mentioning victims of domestic violence and undocumented immigrants as being entitled to relief based upon the sharing of their facial and other information with seemingly anyone who would pay for it, including law enforcement.⁷²

Under all state laws and private organization standards,⁷³ encryption (scrambling) of sensitive information in transit and in storage is recognized as at least highly desirable, if not formally required.

VI. FTC RULES AND ADMONITIONS—DISCLOSURE–BASED AND OTHER

The FTC has emphasized conformance to posted policies to the extent that the greatest exposure for companies is to provide false assurances such as ‘we don’t sell your information’ when someone does so, or ‘your information is perfectly safe with us’ when it is simply impossible for anyone to provide such

70. See *infra* note 167.

71. *Facebook Judge Rips \$550 Million Biometric Privacy Deal*, LEXISNEXIS, (June 4, 2020), <https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.law360.com%2Farticles%2F1279996%2Ffacebook-judge-rips-550m-biometric-privacy-deal&data=02%7C01%7Cmartin.robins%40fisher-broyles.com%7C0acd7364366b4c7a805908d8094bb961%7C9e8fa05ee48847f48de9cd9bd0adf758%7C0%7C0%7C637269568129582479&data=BWQwOn%2Bd8FW5kYZPgKCVyUQyEP%2FCMP7i1AFO6NL%2BIU%3D&reserved=0>.

72. Complaint, American Civil Liberties Union et al. v. Clearview AI, Inc., Ill. Cir. Ct. (2020) (No. 9337839).

73. Such as the National Institute of Science and Technology. *NIST Links Federal Encryption Testing to International Standard for First Time*, NAT’L INST. OF STANDARDS AND TECH, (April 30, 2019), <https://www.nist.gov/news-events/news/2019/04/nist-links-federal-encryption-testing-international-standard-first-time>; see also Karen Scarfone, Murugiah Souppaya, Matt Sexton, *Guide to Storage Encryption Technologies for End User Devices*, NAT’L INST. OF STANDARDS AND TECH, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-111.pdf>. As for the desirable/not formally required distinction: CCPA, for example, has a private right of action for breaches of “nonencrypted or unredacted or nonredacted” personal information. 1798.150(a)(1). (If encrypted, it’s not a breach.) Such is the case as well with New York’s SHIELD Act—the definition of personal information subject to the law is unencrypted data.

assurances. The FTC states directly: “Think your company doesn’t make any privacy claims? Think again — and reread your privacy policy to make sure you’re honoring the promises you’ve pledged.”⁷⁴

While there are numerous FTC enforcement actions based upon this edict,⁷⁵ perhaps the most notable is the ongoing Facebook case beginning with a 2012 Consent Order requiring conformance⁷⁶ and culminating in a 2019 \$5 billion fine for disregard of obligations under the earlier Order.⁷⁷ Customarily, FTC Consent Orders have a 20-year term and require improvement efforts. For example,

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.⁷⁸

While deceptive practices are the customary focus of FTC action, the agency will sometimes address problems not involving deception, such as breaches resulting from the use of obsolete technology under the ‘unfair’ prong of ‘unfair or deceptive trade practices.’ The most prominent example is the TJX episode,⁷⁹ where the issue was a large data breach resulting in substantial consumer loss, apparently resulting from the transmission of consumer data within and from retail stores over a wireless network which was based upon something other than the most recent protocol.⁸⁰ The FTC’s involvement in

74. *Consumer Privacy*, FEDERAL TRADE COMMISSION, <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/consumer-privacy>, (last visited Sept. 13, 2020).

75. *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015). The *Wyndham* case is in a sense the best example. However, the fact that it involved formal federal court action instead of a consent order and involved outright disregard of three data breaches in the face of a privacy policy containing broad assurances of security, makes the case something of an outlier.

76. *FTC Approves Final Settlement with Facebook*, FEDERAL TRADE COMMISSION, (Aug. 10, 2012), <https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook>.

77. While the FTC and Facebook have in fact reached a settlement, at this writing, the settlement is still under consideration by the courts, in part because of the scope of the release. Ryan Tracy & Emily Glazer, *Landmark Facebook Settlement Still Working Its Way Through Court*, WALL ST. J., (Jan. 10, 2020), https://www.wsj.com/articles/landmark-facebook-settlement-still-working-its-way-through-court-11578652202?mod=hp_lead_pos4.

78. *The TJX Companies, Inc.*, FTC Matter/File No. 072-3055, (March 27, 2008).

79. *Id.*

80. 73 Fed. Reg. 18281 (Apr. 3, 2008).

important means of both reducing the likelihood of a problem such as a data breach and demonstrating good faith if and when one does arise.

A separate source of informal guidance in this area is the Federal Communications Commission (“FCC”) in its capacity as regulator of mobile phone carriers. Specifically, the FCC has taken steps to ensure that such carriers provide proper disclosure of, and obtain meaningful consent to, the tracking of users’ whereabouts through GPS and similar geo-location capability built into phones and not sell such information to data brokers at all.⁸⁵ As noted below, addressing location tracking in privacy policies is essential but must be done in conjunction with the FCC’s position. In that such technology is seen by many⁸⁶ as a key part of the strategy for control of pandemics and epidemics, and is already being used for that purpose by a number of governments,⁸⁷ the authors anticipate further attention from other agencies.

In the same vein is the recent report of the US Securities and Exchange Commission discussing what it has observed as the optimal security practices at financial services firms which it audits.⁸⁸ While these observations clearly are not law, they are yet another example of prudent steps that companies should consider. Notably, they have nothing to do with regulation of permitted uses of information by such firms, but are only thoughts on how best to protect it from unauthorized access.

VII. CHILDREN’S ONLINE PRIVACY PROTECTION ACT (“COPPA”)⁸⁹

Enacted in 1998 and, to this day, the only federal statute dealing with limiting the ability of marketers to directly or indirectly track and utilize the online activities of Americans, the text of this law is remarkably sparse and vague. Applicable to web activities of children under 13, it calls for ‘verifiable parental

85. Jon Brodtkin, *Verizon and AT&T will stop selling your phone’s location to data brokers*, CONDÉ NAST, (June 19, 2018), <https://arstechnica.com/tech-policy/2018/06/verizon-and-att-will-stop-selling-your-phones-location-to-data-brokers/>.

86. See *infra* notes 155-161 and accompanying discussion; See comments *infra* note 167.

87. Schechner et al., *Tech Firms Are Spying on You. In a Pandemic, Governments Say That’s OK*, WALL ST. J., (June 15, 2020), https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths11592236894?emailTo-ken=9e1d763d10ae1df9221c3e70debbe47ciXV4JuTxS22Wj/srwFVOGIQPrTUbnD4XlFOQqObPzMDqTAE7TXluP2v0aX33CkPasWuVRKsHSeFfpjVyUvthk3aIdKD44ePI2tH0pcfKZRY9prU-girgCOBt7jdg1z5kewKFboyP1hLsV0R3wWDVKgQ%3D%3D&reflink=article_email_share. One wonders how this activity is viewed by the FCC.

88. Press Release, SEC, SEC Office of Compliance Inspections and Examinations Publishes Observations on Cybersecurity and Resiliency Practices (Jan. 27, 2020), <https://www.sec.gov/news/press-release/2020-20>.

89. 15 U.S.C. §§ 6501-6505; 16 C.F.R. § 312 et seq.

consent’ for data collection in the case of ‘websites or online services’ directed to ‘children’:

The term “verifiable parental consent” means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator’s personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from that child.

...

The term “website or online service directed to children” means-

- (i) a commercial website or online service that is targeted to children;
- or
- (ii) that portion of a commercial website or online service that is targeted to children.⁹⁰

A good deal is left to the interpretation of marketers—i.e., ‘reasonable efforts,’ ‘targeted to children’—who unsurprisingly have taken liberties with the law, a tendency exacerbated by a lack of regulatory attention which seems to be rapidly changing. The FTC has appropriately recently responded with enforcement action via a \$170 million settlement in a case involving Google’s YouTube subsidiary and allegedly blatant abuse, where salespeople were openly promoting their site as the best way to reach children⁹¹ which bespeaks the increasing significance of the law.

In addition to the fine, the settlement also required operational changes such as:

- limitation of data collection from anyone watching children’s videos;
- modification of features appearing on such videos such as comment, live chat, and saving to playlists;
- omission of ads from children’s videos which are served based upon online activity; and

90. 15 U.S.C. §§ 6501(9), (10).

91. *Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law*, FEDERAL TRADE COMMISSION, (Sept. 4, 2019), <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>.

- requiring video producers to designate videos as being for children or adults.⁹²

While nebulous and perhaps somewhat dated references such as ‘online services’ and the ambiguity of the terms noted above complicate efforts to apply the statute in all of the situations where it is most needed, it is still a significant consideration with respect to marketing efforts directed to younger people and must not be ignored.⁹³ It must be emphasized that COPPA does not preempt any other state or federal law, all of which must be observed to the extent applicable.

Whether Google or YouTube actually changed its practices as a result of the \$170 million settlement of the FTC case discussed earlier in this section is unclear. In the second quarter of 2020, an Illinois resident brought suit seeking class action status against Google in California alleging violations of COPPA and the Illinois biometric statute⁹⁴ resulting from Google’s provision of free Chromebook machines to schoolchildren and alleged programming of these machines to surreptitiously track internet activity and perform facial scans.⁹⁵

At this writing, a bill sponsored by Sens. Hawley and Markey (the latter of whom was the primary sponsor of the original COPPA) is pending in Congress, although prospects are clouded by the COVID-19 situation. Said bill would maintain parental consent for the collection of data of children under 13, add a new prohibition on the collection of information of children ages 13-15 years without such users’ consent, and make several of the other changes contemplated herein.⁹⁶

92. Natasha Singer, *How YouTube Is Changing its Approach to Child Privacy*, N.Y. TIMES, January 7, 2020, at B4.

93. See *infra* notes 143-144 (containing the authors’ thoughts as to improvement of the statute).

94. 740 ILL. COMP. STAT. 14 (2008) et seq.

95. Hayley Samsel, *Google Facing Lawsuit Over Collection of Facial Scans, Personal Data From Children*, 1105MEDIA INC., (April 7, 2020), <https://securitytoday.com/articles/2020/04/07/google-facing-lawsuit-over-collection-of-facial-scans-personal-data-from-children.aspx>. As an additional example of the spotty enforcement of COPPA, a respondent is accused of falsely stating that it was participating in a self-regulatory organization. *FTC Dem Says Kids’ Privacy Programs Need More Scrutiny*, LEXISNEXIS, (May 19, 2020), <https://www.law360.com/articles/1275121/ftc-dem-says-kids-privacy-programs-need-more-scrutiny>. The same source also indicates the bipartisan interest in improvement.

96. Press Release, U.S. Sen. Ed Markey, Senators Markey and Hawley Introduce Bipartisan Legislation to Update Children’s Online Privacy Rules (Mar. 12, 2019), <https://www.markey.senate.gov/news/press-releases/senators-markey-and-hawley-introduce-bipartisan-legislation-to-update-childrens-online-privacy-rules>. The United Kingdom has very recently enacted a GDPR-style law to deal with efforts pertaining to children. As is the case with COPPA, observers note that the law requires ‘a lot of judgment calls’ to be made. *UK Extends Privacy Law Patchwork With New Kids’ Rules*, LEXISNEXIS, (Jan. 24, 2020), <https://www.law360.com/articles/1237351/uk-extends-privacy-law-patchwork-with-new-kids-rules>.

VIII. CALIFORNIA CONSUMER PRIVACY ACT (“CCPA”)⁹⁷

By far the most comprehensive US legislation dealing with information usage, CCPA became effective at January 1, 2020. At this writing, there has been no formal judicial guidance as to its application.⁹⁸ While it is the closest thing in US law to the GDPR, there are substantial differences.⁹⁹ Most notably, these include a broader definition of personal information through inclusion of a ‘household’ component, lack (at least nominally) of a general opt-in requirement, the incorporation of the DO NOT SELL opt-out mechanism, and a requirement pursuant to legislation separate from but related to CCPA for data brokers to register with, and provide information to, the California Attorney General.¹⁰⁰ CCPA applies to both consumers and business to business transactions, but with a partial exemption until January 1, 2021 for the latter.¹⁰¹

Some believe, with reasonable basis,¹⁰² that the legislation was enacted in large part to deal with the purported scandal associated with delivery of Facebook information of millions of users to a UK professor in contravention of Facebook’s assurances and the subsequent use of such information in the 2016 US presidential campaign. This brought a spotlight to the involvement of intermediaries (middlemen) such as data brokers and aggregators. In addition to the data broker registry requirement,¹⁰³ the statute gives consumers self-help tools, which include:

A consumer shall have the right to request that a business that collects a consumer’s personal information disclose to that consumer the categories and specific pieces of personal information the business has collected.¹⁰⁴

97. CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020).

98. However, there have been promulgated final regulations. Cal. Code Regs. tit. 20 § 999, <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-reg.pdf>

99. *CCPA vs. GDPR*, WORKTABLE TECH. LTD., <https://resources.workable.com/hr-terms/ccpa-vs-gdpr>, (last visited Sept. 13, 2020).

100. Assemb. B. 1202, 2019, Reg. Sess. (Cal. 2019).

101. Amy S. Park & Aylin Kuzucan, *An Amendment to the CCPA Provides a Welcome But Brief Reprieve for B2B Businesses*, ALM MEDIA PROPERTIES, LLC, (Oct. 25, 2019), <https://www.law.com/therecorder/2019/10/25/an-amendment-to-the-ccpa-provides-a-welcome-but-brief-reprieve-for-b2b-businesses/>.

102. Dipayan Ghosh, *What You Need to Know About California’s New Data Privacy Law*, HARV. BUS. REV., (July 11, 2018), <https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law>.

103. Cal. Assemb. B. 1202.

104. CAL. CIV. CODE § 1798.100 (West 2020).

A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.¹⁰⁵

A consumer shall have the right to request that a business that sells the consumer's personal information, or that discloses it for a business purpose, disclose to that consumer:

- 1) The categories of personal information that the business collected about the consumer.
- 2) The categories of personal information that the business sold about the consumer and the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold.
- 3) The categories of personal information that the business disclosed about the consumer for a business purpose.¹⁰⁶

A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This right may be referred to as the right to opt-out.¹⁰⁷

There are many components of the legislation,¹⁰⁸ only a few of which are quoted above, but in the authors' view, the most important ones are as follows:

- Broad application outside California: the law applies to any for-profit entity ("business") (i) with aggregate global revenue in excess of \$25 million,¹⁰⁹ (ii) that obtains the personal information (as defined in the act) of more than 50,000 California residents, or (iii) that derives 50% or more of its revenue by selling (as defined in the

105. CAL. CIV. CODE § 1798.105(a) (West 2020).

106. CAL. CIV. CODE § 1798.115 (West 2020).

107. CAL. CIV. CODE § 1798.120 (West 2020).

108. *California Consumer Privacy Act (CCPA)*, CAL. DEP'T JUST., <https://oag.ca.gov/privacy/ccpa>, (last visited Sept. 13, 2020) (containing an official Attorney General summary).

109. Some have suggested that the failure to limit application to companies with California-derived revenue in excess of the threshold is a drafting error. Perhaps this is the case, but the actual language does not presently support such conclusion and the only sensible position to be taken at this time is what is dictated by the actual language, namely all revenue is taken into account. Further, the California Attorney General had the opportunity to clarify this point, but chose not to do so, in the draft regulations and on the CCPA Fact Sheet. *California Consumer Privacy Act (CCPA)*, CAL. DEP'T JUST., https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf (last visited Sept. 23, 2020).

act) the personal information of California residents. The final prong is one which, in the authors' experience, sometimes ensnares very small companies that process data of a relatively low number of consumers, in which case the application of CCPA is out of step with the apparent intent of the statute to protect consumers in substantial numbers;

- A requirement, similar to that of the GDPR, for clear, non-legalistic disclosure in privacy policies and elsewhere of what information is being collected, what is being shared, with whom, and why.¹¹⁰ The drastic increase in the use of the Zoom video conferencing service during the COVID-19 outbreak prompted at least two class action lawsuits by users, challenging the sufficiency of the disclosures in light of allegedly undisclosed provision of user information to Facebook;¹¹¹
- An ambiguous provision not found in the GDPR, intended to allow consumers to opt out of 'sales' of their information through mandatory inclusion on websites and in mobile applications of a DO NOT SELL button and, in some cases not involving a California physical location or direct connection to California consumers, a toll free phone number. However, this provision leaves open to interpretation by courts and in regulations¹¹² whether a sale includes transfers to third parties such as web hosts, fulfillment vendors, and analytics vendors absent direct monetary remuneration; the

110. To some extent, this notice requirement is being implemented through paper notices to customers in a physical location. Nat Ives, *Privacy Warnings Come to Brick-and-Mortar; Emission Brags will be the Next Big Packaging Play*, DOW JONES CO., https://cmo.createsend1.com/t/ViewEmail/d/484C228B20C823A72540EF23F30FEDED/4B7310DCAEF300FE62AF25ACF5E3F0AC?mod=article_inline&mod=hp_minor_pos1, (last visited Sept. 13, 2020).

111. *E.g.*, Cullen v. Zoom Video Communs., Inc., 2020 U.S. Dist. LEXIS 78745, Case No. 20-CV-02155-LHK (N.D. Cal., April 24, 2020); Taylor v. Zoom Video Communications, Inc., Case No. 20-cv-02170, (N.D. Cal. Mar. 31, 2020) (subsequently consolidated with 6 other class actions). Most of the suits also allege claims associated with failure to safeguard personal information. On the date that this article was finalized, November 10, 2020, Zoom and the FTC agreed to a settlement of charges pending before the latter which provided no monetary relief but committed Zoom - through entry of an injunctive order - to terms which prohibit misstatements as to security practices and data sharing and enhance technical measures such as encryption of stored recordings. This settlement has no impact on any of the private litigation which is pending.

112. CAL. CIV. CODE § 1798.120 (West 2020). A sale is defined in CAL. CIV. CODE § 1798.140 (West 2020) as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party for monetary or other valuable consideration." The 'valuable consideration' portion—among other things—leaves a great deal of room for interpretation.

differences in approach among major internet companies are starkly apparent;¹¹³

- The above ambiguity is compounded by a confusing exception to the DO NOT SELL requirement related to obligations for sharing of data with ‘service providers’;¹¹⁴
- While nominally absent from the statute’s text (in contrast to the GDPR), an opt-in provision is at least part of best practices for establishing adequacy of disclosures; arguably the best way to establish provision of required notices is to point to express agreement to their terms;¹¹⁵
- A prohibition on discrimination—through pricing or otherwise—against those who exercise the DO NOT SELL option;¹¹⁶
- A private right of action for damages attributable to violations in connection with certain unauthorized access and exfiltration, theft, or disclosure of a consumer’s nonencrypted or nonredacted personal information.¹¹⁷

At this very early stage, it is not clear how the law will be enforced. What is clear is that it must be dealt with in privacy policies governing most collection of personal information from California residents.¹¹⁸

113. Kim Lyons, *No one is ready for California’s new consumer privacy law*, VOX MEDIA, (Dec. 31, 2019), <https://www.theverge.com/2019/12/31/21039228/california-ccpa-facebook-microsoft-gdpr-privacy-law-consumer-data-regulation>.

114. For the purpose of the DO NOT SELL exception, a service provider is: (1) A legal entity organized for profit; (2) That processes personal information on behalf of a business; (3) To which the business discloses a consumer’s personal information for a business purpose. (4) Pursuant to a written contract that prohibits the legal entity from selling, retaining, using, or disclosing the personal information for any purpose (including a commercial purpose) other than performing the services specified in the contract. *See* CAL. CIV. CODE § 1798.120 (West 2020) (right to opt out), § 1798.135 (“Do Not Sell” requirement), § 1798.140(d) (definition of ‘business purpose’), § 1798.140(t)(1) (definition of ‘sell’), § 1798.140(v) (definition of ‘service provider’), § 1798.140(w) (definition of ‘third party’). At this writing, there is a stark difference of opinion among major technology companies over the application of this section. Patience Haggin, *Facebook Won’t Change Web Tracking in Response to California Privacy Law*, WALL ST. J., (Dec. 12, 2019), <https://www.wsj.com/articles/facebook-wont-change-web-tracking-in-response-to-california-privacy-law-11576175345?mod=searchresults&page=1&pos=13>. The final regulations issued by California’s Attorney General do not resolve this ambiguity. *As Final Calif. Privacy Regs Drop, Enforcement Fights Loom*, LEXISNEXIS, (June 12, 2020), <https://www.law360.com/articles/1282100/as-final-calif-privacy-regs-drop-enforcement-fights-loom>. Presumably, it will be resolved fairly promptly through legal proceedings of some sort.

115. For those subject to the GDPR’s opt-in requirement, the matter is effectively moot—it is likely to be easier to have all opt in than to present separate approaches to users, based upon their location.

116. It is not clear how this prohibition is applied in cases where sharing of information is essential to proper site or application functionality.

117. CAL. CIV. CODE § 1798.150 (West 2020).

118. *Infra* note 130 and accompanying Appendix text (discussing one company’s equivocal response).

It is also clear that allocation of responsibility for compliance (and liability for non-compliance) will be an important aspect of contractual practice where personal information is involved. The latter will include not only initial collection and sharing activity, but also responsibility for handling of data subject requests. While all sharing of personal information requires careful disclosure, the highest level of scrutiny will go to situations involving some sort of direct monetary or other consideration. It is quite possible that some companies will respond to the CCPA as others have to the GDPR, namely taking technical steps to block access by residents in those jurisdictions. While marketplace considerations will not always permit such action, for some companies having actual and anticipated minimal sales attributable to California, it remains a potential option.

IX. ROLE OF PRIVACY POLICIES

The above authority is translated into action and communication (and sometimes liability) through online and paper privacy policies setting forth how each company obtains and handles user information¹¹⁹ As noted above¹²⁰ the FTC has made non-compliance with one's own policy a focal point of their enforcement activity, so these documents are ultimately contractual in nature.

The policy excerpts contained in the Appendix reflect the typical contents of such documents,¹²¹ both in general and in response to the new dictates of the CCPA. Such items should always include:

- a description of information being collected and explanation of why such materials are needed for the conduct of business;¹²²
- an explanation of what is being done with the information, specifically, with whom it is being shared and for what purpose;¹²³

119. Terms of Use (TOU) documents are usually presented with privacy policy documents, but serve different purposes. TOU's usually contain commercial terms such as sales tax treatment, warranties and disclaimers and return policy and where public submissions are permitted or encouraged, specify what is off limits such as obscene or violent materials or materials which infringe anyone's copyright. The question of screening for untruths or 'fake news' which may impact political races—or even whether to accept political ads at all—is often addressed in this context. For example, Facebook's Community Standards “ban hate speech, harmful content and content designed to intimidate voters or stop them from exercising their right to vote.” Emily Glazer, *Facebook to Keep Targeted Political Ads but Give Users More Control*, Wall St. J., (Jan. 9, 2020), https://www.wsj.com/articles/facebook-to-keep-targeted-political-ads-but-will-give-users-more-control-11578567603?mod=hp_lead_pos6.

120. FEDERAL TRADE COMMISSION, *supra* note 74.

121. Which must always reflect actual and intended practice.

122. Appendix Sections A–C.

123. Appendix Section D.

- a disclosure of website activity monitoring;¹²⁴
- either in the policy itself or related disclosure (such as a ‘cookie banner’ that appears when a site or application is first accessed), statement regarding use of persistent ‘cookies’ which are computer code files placed on user equipment which may allow user tracking across sites; their use is becoming increasingly controversial and being phased out in some quarters;¹²⁵
- potential or actual use of such information for targeting of advertising by third parties;¹²⁶
- an explanation that no complete assurance can be given as to the maintenance of security for the information;¹²⁷ and
- merger and acquisition disclosure¹²⁸ dictated by state Attorney General Accord in Radio Shack bankruptcy case.¹²⁹

For companies meeting the CCPA thresholds, the other disclosures regarding actual or potential ‘sales’ come into play. In the materials provided, the company uses something of a hybrid approach to deal with the uncertainty around whether a sale encompasses transfers not involving monetary consideration. For example, while there is a ‘Do Not Sell’ home page link, which is required when there is a sale,¹³⁰ the reference in the policy to that link, which is also required under the statute, is not labeled ‘Do Not Sell’ but rather as an ‘opt-out’ of ‘sales.’

The best examples of genuine sales for which the DO NOT SELL election is pertinent involve data brokers who openly trade in databases possessing demographic or other characteristics which are believed to facilitate the marketing efforts of their customers. When such parties are involved, very strong disclosures are essential.

The California-specific language also reflects the ability of consumers to know what information has been collected with respect to them and to insist upon cessation of such collection.¹³¹

124. Appendix Sections C & E.

125. Bowdeya Tweh & Sahil Patel, *Google Chrome to Phase Out Third-Party in Effort to Boost Privacy*, WALL ST. J., (Jan. 14, 2020), https://www.wsj.com/articles/google-chrome-to-phase-out-third-party-cookies-in-effort-to-boost-privacy-11579026834?mod=lead_feature_below_a_pos1. The title of the article reflects Google’s decision to eliminate the ability of third parties to use its Chrome web browser to place cookie code on user devices.

126. Appendix Sections B & C.

127. Appendix Section H.

128. Appendix Section I.

129. Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 742, 783 (2016).

130. Appendix Section G.

131. Appendix Section F.

While the Appendix reflects steps taken to comply with the CCPA, it is not tailored to companies which are subject to the GDPR. Policies for such companies would have, *inter alia*, GDPR specific disclosures about data subject requests (including the right to complain to a regulatory authority),¹³² disclosures of the legal basis for the processing of the personal information, and mechanisms for providing opt-in consent to indicate their agreement.

X. CRITIQUE AND RECOMMENDATIONS: GENERAL AND RESPONSIVE TO COVID-19 DEVELOPMENTS

Any evaluation of an existing or proposed legal regimen must address four questions:

- What harm is to be ameliorated by virtue of such intervention?
- Can and will private markets do the job more efficiently?
- Is the solution being evaluated actually contributing to improvement?
- What governmental unit(s) are best suited to implement regulation which is otherwise called for?

Based upon the gravity of several of the measures which have been proposed to deal with COVID-19, the authors believe that separating the discussion of such measures from discussion of existing law is the best way to evaluate both.

A. Breach Notification Statutes

The easiest analysis is with respect to laws requiring breach notification. There is a clear need to take steps to reduce financial fraud resulting from data breaches. One way to do so is to introduce penalties for companies which do not assist consumers in this regard, while the other is to provide consumers the information needed to assist themselves. The numerous data breaches occurring in recent years¹³³ bespeak the actual—not potential—consumer exposure. Criminals would not engage in this activity if it were not beneficial to them. While some companies would take appropriate steps when being apprised of a problem, the delayed issuance of public notices that is all too prevalent indicates that this is not necessarily the case.

132. GDPR, *supra* note 3, at article 13.

133. Green et al., *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER, (Nov. 19, 2019), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1#macys-1> (indicating at least 19 consumer data breaches since January 2018). Many more, such as Barnes & Noble, Chase, Yahoo, and Home Depot, just to name a few, occurred prior to such date.

Both anecdotal and empirical¹³⁴ indicia reflect the actual inconvenience and harm to consumers. While there is no way to determine what harm would have resulted if consumers were not advised of their exposure from breaches that did occur, or how many breaches did not occur because of security measures taken by companies seeking to avoid notice obligations, common sense indicates that the answer is far more than zero. That is, the breach notices do result in reduction of consumer harm. Absent notice of breaches, there is relatively little that impacted consumers can do to reduce their risk.

The requirements which the authors have observed associated with these breach notification laws are also not overly burdensome. For those not experiencing breaches, the obligation is largely that of development of an incident response plan, which, while not trivial by any means,¹³⁵ is not horrendous. In any event, for multi-national companies, such plans are dictated by Art. 32 of the GDPR, so the incremental burden associated with US law is very low.

Even when a breach does occur, the required steps, such as written notice and offering of credit monitoring services, have become mainstream and, while usually costly, are not a major operational disruption.

The above analysis militates strongly in favor of such regulation, but the patchwork of state laws is a problem. The potential harm to a consumer from a data breach is the same whether the consumer resides in France, California, or North Carolina, so there is no reason for varying state standards. There is a burden to business associated with having to track varying ‘triggers,’ notice time frames, and nuances in notice forms and procedures. This is not a situation where the use of states as an innovation laboratory serves any purpose, and the irony is that each state’s zeal to legislate in this area has contributed to the exercise that undermines the very protections the statutes seek to afford.¹³⁶ The patchwork approach benefits no one, but instead makes it harder for affected businesses to get necessary information to individuals on a timely basis. A uniform federal standard is sorely needed.

134. Dan Swinhoe, *The 15 biggest data breaches of the 21st century*, IDG COMM’NS, INC., (April 17, 2020), <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>.

135. Robins et al., *Privacy and Information Security – Cyber Incident Response Planning*, FISHERBROYLES LLP, (Mar. 28, 2017), <https://www.lexology.com/library/detail.aspx?g=71150f7e-2525-49ca-bccd-431445aca06c>.

136. One of the authors, who advised a client on an actual data breach response several years ago when the statutory framework was less complex, observes that the research to determine the various requirements in each state where there was an affected individual took a substantial amount of time which delayed the actual notification process, which could have been better spent by the impacted individuals in self-help efforts to investigate and mitigate harm.

B. State Substantive Regulation

While there is a very strong case to be made for breach notice laws, the same cannot be said for the efforts of states (and even the FTC) to prescribe technology and practices intended to secure information. The fundamental problems with such steps are that (i) they may cause the entrenchment of obsolete approaches and technology, and (ii) the approaches of the various states may be inconsistent with each other and/or the FTC. With technology changing so rapidly, literally several times per year in many relevant cases, what seems to be state of the art practice today may prove to be undesirable in short order. Fixing technical requirements by reference to a particular point in time (such as requiring encryption at a given number of ‘bits’) will seriously exacerbate the problem. In any event, it is difficult to understand how legislators—at any level—can grasp the nuances of different approaches. Even if they could do so, it is inevitable that issues will be seen differently by different people, which may lead to inconsistency. Perhaps worse yet is the possibility that protocols endorsed or required by such laws will become targets for criminals.

While the risk of inconsistency militates in favor of such regulation being implemented at the federal level, if it is to be done at all, the authors do not recommend that it be done at all. The FTC’s effort to hold a company liable for use of N-1 generation wireless technology in the *TJX* case¹³⁷ is a good example. Surely, in 2020 and beyond, we do not want there to be any inference that any technology which was suitable in 2006, 2008 or even 2018 is currently suitable. It is far better to hold companies accountable for results, as opposed to prescribing specific technological steps to be taken.

C. Informal FTC Regulation

The informal FTC regulation is quite interesting. On the one hand, the FTC has usually taken a sophisticated, nuanced approach and developed insightful guidance for business. While any particular pronouncement can be the subject of debate, most knowledgeable observers would agree that on balance, the FTC is performing a real service to the public and the business community with its real world-based suggestions for problem avoidance. This is why the authors emphasize such guidance in day-to-day counseling activity. The ongoing plethora of data breaches suggests that marketplace competition will not mitigate the problem. Consumers for the most part do not have the expertise to distinguish among responsible and irresponsible vendors, and they have no visibility¹³⁸ or

137. *The TJX Companies, Inc.*, FTC Matter/File No. 072-3055, (March 27, 2008).

138. GDPR addresses this issue of visibility and requires that processors disclose and obtain from the controller authorization for all third parties who process the data of the controller downstream. GDPR, *supra* note 3, at article 28. The proposed California ballot initiative entitled Consumer Privacy

control into the third party providers that support the vendors with whom they interact, such third party providers having an equally important role in privacy and data security.

On the other hand, the characterization of such guidance as merely informal is problematic in light of the absence of precedential value of the consent decrees and Orders beyond the stated parties. There is also a question of sanctions applicable to other parties who fail to take their cue from the directives. If the FTC's direction is in the public interest, it should be actual law. If it is merely 'helpful guidance' but not mandatory, this should be made clear. It is hard to see how anyone benefits from this level of uncertainty. A businessperson can quite reasonably ask in response to the invocation of the FTC's guidance, 'is this the law or isn't it?' Especially where conformance to the FTC's direction will involve a substantial financial and operational burden, which is often the case for smaller and medium sized clients in industries not customarily thought of as data intensive, this determination is a key part of job performance for those responsible for legal compliance. Government by press release and pamphlet is not government at all.

While the only court to take up the matter has affirmed the FTC's authority to act in this manner,¹³⁹ the promulgation of so many specific directions pursuant to a general 1914-era statutory prohibition of unfair or deceptive trade practices gives pause to most observers¹⁴⁰ and allows questions as to the eventual position of other courts, ultimately including the US Supreme Court. Not surprisingly, the current FTC Chairman, Joseph Simons, has strongly advocated for some sort of codification.¹⁴¹

As is the case with breach notification, it is time for Congress to speak either through formal endorsement of these positions or a codification of specific topics and rejection of others.

D. Children's Online Privacy Protection Act

As to COPPA, there is little dispute as to the need for oversight of the tracking of activity of children, who are inherently unable to properly oversee their

Rights Act seeks to amend the CCPA by requiring service providers and contractors (a new definition) to provide notice of the use of other persons used to process personal data of the business. California Public Records Act of 2020, Sec. 14 (amending CAL. CIV. CODE §§ 1798.140(ag)(2), 1798.140(j)(2) (West 2020)).

139. *FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D. N.J. 2014).

140. Robins, *supra* note 23 (discussing the opinion of Former Homeland Security Secretary Chertoff).

141. Eric J. Savitz, *The Chairman of the FTC Says We Need a Federal Privacy Law*, DOW JONES CO., (Jan. 7, 2020), <https://www.barrons.com/articles/ces-ftc-chairman-privacy-law-51578436640>.

own affairs. This is another situation where a national standard is in order as children's exposure is the same regardless of geography. COPPA is a good starting point for such standard, but only a starting point.

While it is appropriate for the FTC to demonstrate that the statute is not a dead letter by going after those who blatantly disregard its existence,¹⁴² this will not suffice. Among other needs is an amendment of the statute to remove some of the ambiguity created by terms such as 'directed to children' and substitute a new standard that may be tied, for example, to a given amount of actual usage by children,¹⁴³ the site's acceptance of advertising of particular types of products, or whether the site is operated by a vendor of products used primarily by children. Another approach may be to regulate the transfer or other use of data by requiring some sort of certification in connection with the transfer as to the good faith lack of awareness, following reasonable inquiry, of the inclusion of such child-centric data in what is being transferred. There is no foolproof way of excluding all children from sites which are the subject of tracking efforts, but requiring greater vigilance is definitely in order. Clarifying legislation should incorporate several of the terms of the YouTube settlement¹⁴⁴ and perhaps the new UK law.¹⁴⁵

E. Information Collection and Usage; Present law: Opt-in; Opt-out

While measures to prevent or mitigate fraud and protect children are certainly in order notwithstanding the issue of from where they should emanate, the matter of 'pure' privacy regulation for adults which is not associated with fraud prevention is different. One must ask 'what harm is ultimately at issue with such regulation?' Perhaps the better question is 'what is meant by harm?' While there is much to be said for, and little to be said against, taking substantial steps to prevent and mitigate financial fraud, it is worth asking about the wisdom of the premise of the GDPR and CCPA that the simple collection and sharing of even 'benign' personal information like an IP address is in itself harmful.¹⁴⁶ One can reasonably argue the philosophical merits of both positions, but in the authors' view the absence of tangible, discernable harm dictates a rigorous consideration of the costs and benefits associated with more stringent regulation of commercial data collection and use.

142. FEDERAL TRADE COMMISSION, *supra* note 91 (noting that it (the FTC) has done so in the *YouTube* case).

143. Although the mechanics of determining the age of a user are sometimes daunting.

144. *See* Singer, *supra* note 92.

145. U.S. Sen. Ed Markey, *supra* note 96.

146. Such harm, to the extent it exists, can usually be mitigated through user action such as adjustment of device settings to enable private browsing mode, among other things, and express requests to stop communications.

The common explanation/rationale for such regulation is the provision of people's internet activity profiles to third parties without their consent, but this begs the question: what is the harm in that? Such action often leads to serving of targeted advertising based upon a person's web browsing history or physical location triggering promotional contact. Such advertising may take the form of political advertising as was the case in the Cambridge Analytica situation.¹⁴⁷ However, no one is forced to respond to such advertising, whether by purchasing the subject products, voting as desired, or otherwise. Regardless of whether one likes it, it is virtually impossible to avoid being served often irrelevant advertising in public spaces. At least the use of targeting techniques has the potential benefit of making an effort to appeal to individual preferences and is a major component of the 'free' internet. For that matter, no one is forced (or fraudulently induced) to join platforms such as Facebook. As noted above, there is good reason for concern about children being deceived or enticed into dangerous situations, but by definition, adults are considered to be capable of properly exercising discretion.

Simply put, deterring targeted advertising of any kind—commercial, political or other—does not seem to implicate the individual freedom concerns that are so often cited as the basis for this type of regulation and which are discussed *infra* in the separate COVID-19 discussion section. This is the case whether the advertising results from the use of cookies, geolocation tracking to facilitate serving of targeted advertising by businesses in the individual's current vicinity, or other devices. None of this has anything to do with information provision to, or usage by, government. If anything, a recent data breach indicates that Americans may be better protected by extension of the existing regulatory focus on securing the data used for such activity than by limiting its collection or use.¹⁴⁸

An example of the juxtaposition of these rationales is found in an unlikely place, namely an interview with Washington Post technology columnist Geoffrey Fowler.¹⁴⁹

Mr. Fowler "dissects the privacy policies and practices of some of the world's biggest, most powerful and most influential companies, and challenges

147. Alex Hern, *Cambridge Analytica: how did it turn clicks into votes?*, THE GUARDIAN, (May 6, 2018 03:00 EDT), <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>.

148. Zack Whittaker, *Oracle's BlueKai tracks you across the web. That data spilled online*, TECHCRUNCH, (June 19, 2020), <https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/>.

149. Jacob Sweet, *Your Tech Relationship Counselor: Geoffrey Fowler tackles the "great reckoning" with privacy*, HARV. MAG., January–February 2020, <https://www.harvardmagazine.com/2020/01/geoffrey-fowler-tech>.

them to do better. . . . [H]e uses brand new credit cards from Amazon and Apple to buy a single banana from Target then tracks how the two industry giants broadcast his data to a host of private companies.”¹⁵⁰

Again, so what harm has been done? Nothing forces Mr. Fowler to do business with any of the recipients. Some might consider this sort of sharing and follow-up to be ‘creepy,’ an adjective that surprisingly has been used somewhat as a term of art in the industry, but that begs the question of whether they cause any actual harm, and if so, what kind and to what extent.

In the same article and on the same page, Mr. Fowler exhibits the same confusion as so many observers and commentators when he ‘sees potential danger when governments have more tools to harness data’¹⁵¹ and refers to the efforts of Hong Kong protestors to shield their identities. The concern with governmental surveillance is a legitimate one and has taken on greater significance as society grapples with the best way to manage and mitigate COVID-19¹⁵², but there is no effort to make a connection between sharing by commercial parties and such surveillance. A reference in the concluding paragraph to “surveillance capitalism” further muddles the issue.

From recent experience with CCPA and GDPR client compliance efforts, the authors can say that there is a good deal of burden and expense associated with such process. Among other things, this includes redrafting of privacy policies, working with web hosts and designers to incorporate election boxes, data mapping and cookie banner inclusion, providing for retention of records of such information for use in connection with investigations or litigation, working with staff to handle data subject requests and putting in place with third party vendors appropriate (and generally highly negotiated, often by outside counsel) covenants,¹⁵³ warranties and indemnities, and procurement of dedicated insurance coverage. What is not always apparent is that virtually any web presence involves sharing of information with required infrastructure vendors such as

150. *Id.*

151. *Id.*

152. Revelations regarding use by the US Internal Revenue Service of GPS tracking data to pursue those suspected of criminal tax violations only enhances such concerns and adds credence to those of Mr. Snowden. Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J., (June 19, 2020), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815?emailTo-ken=9e9d44a7c86e3c112b94eaa5c357dd831CglupjbrzWuWeGkLzwF0xjIKwyB6uoIdqmvDZ-KoyRAJRFgmlFM/XR2Omwp9tYir/645KAm4MVlhiWXkJN14G3jhMIkiGcabx54EtgP746nLKaARyCwVFoc7z+t/as6P&reflink=article_email_share.

153. For GDPR and CCPA, the detailed prescriptions around such requirements necessitate amendment of contracts even where the existing language provides for the substance of the requirements. GDPR, *supra* note 3, at article 28; CAL. CIV. CODE § 1798.140(w)(2)(A) (West 2020).

hosting providers, even where no one is making any surreptitious effort to sell anything to or otherwise influence data subjects.

It is difficult to accept the need for burdensome legislation simply to ‘protect’ people against sales or persuasion efforts which are presented in many other contexts which are not mitigated through such legislation. Very simply, in a capitalist, democratic society, the premise is that adults can and should make their decisions as to purchases or votes without government prompting. If there is a case to be made for legislation to avoid government surveillance, it should be made directly and not through the use of a red herring involving commercial solicitations.

Even Edward Snowden questions the value of the GDPR (and presumably would question the value of the CCPA) in responding to the privacy and surveillance concerns that prompted him to speak out.¹⁵⁴ While his concern is admittedly with the insufficiency of the sanctions, he openly questions whether the ultimate issue is collection of the sensitive data in the first place, as opposed to endorsing doing so pursuant to supposedly express consent. Whatever Mr. Snowden may think, the authors have difficulty seeing the privacy benefit associated with the elaborate mechanical steps dictated by the GDPR and CCPA. Imposition on private companies of these requirements for mechanical steps does nothing to prevent or regulate government surveillance which, as discussed *infra* in the context of COVID-19 response measures, is of much greater significance now than was the case when the CCPA and GDPR were enacted.

Making such laws even more problematic is their imposition in patchwork fashion. The considerations are the same regardless of data subject location, and the various requirements simply complicate compliance efforts. If requirements are in order at all within the US, they should be created at the federal level.

XI. COVID-19 AND PRIVACY

The preceding discussion of existing authority hopefully prompts consideration of several major topics associated with the role and scope of existing privacy law and related technology in American law and society. However, COVID-19 and various measures, which are contemplated to deal with and prevent its spread, implicate these and other considerations in a different and quite impactful manner and warrant separate discussion. Everyone within and outside the public health area agrees that early detection and contact tracing of those who are infected or are likely to become infected are—perhaps the

154. Steve Ranger, *GDPR is missing the point, says Edward Snowden*, ZDNET, (Nov. 4, 2019), <https://www.zdnet.com/article/gdpr-is-missing-the-point-says-edward-snowden/>.

most—important tools in the effort to combat the virus, at least until development of an effective vaccine and perhaps even thereafter.

A. *Alternative Technologies*

The technology to carry out such detection and tracing exists and, while continuously being refined, the US has deployed such technology at a surprisingly slow pace.¹⁵⁵ Among other things, it uses location tracking technology, the limited usage for this purpose by governments leveraging data generated by private firms is discussed,¹⁵⁶ and sometimes Bluetooth key overlap analysis,¹⁵⁷ and possibly other aspects of someone’s electronic footprint such as payment card transactions, to determine whether a person has come into potentially close-contact with someone who has tested positive for the virus, as well as whether someone who has the virus has been spreading it. Such technology is integrated into smartphone apps presently available for download, and attorneys general across the US have raised concerns that the apps are proliferating without adequate restrictions to protect individuals’ privacy.¹⁵⁸

B. *Voluntary vs Mandatory: Legal and Health Ramifications*

Present and potential revision in US privacy law becomes relevant with respect to whether persons simply may or must download the app and what is done with the information which it generates. Many people, presumably including most of those at high-risk of complications from the virus, will eagerly procure the app and utilize its information for early detection so that they may have as much warning as possible of potential infection and take preventative

155. Associated Press, *Contact tracing apps are off to a slow start in the U.S.*, NBC News, (May 19, 2020), <https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.nbcnews.com%2Ftech%2Ftech-news%2Fcontact-tracing-apps-are-slow-start-u-s-n1210191&data=02%7C01%7Cmartin.robins%40fisher-broyles.com%7C39a59e550a7346c4959708d80cb075fc%7C9e8fa05ee48847f48de9cd9bd0adf758%7C0%7C0%7C637273299326600648&data=C2rOq%2BjWzLLErexcn8s4st4Xm%2F5QOa%2F0YnCd9ZnL5qc%3D&reserved=0>.

156. Complaint, American Civil Liberties Union et al. v. Clearview AI, Inc., Ill. Cir. Ct. (2020) (No. 9337839). Whatever the exigency of the situation may dictate, current usage seems to fly in the face of at least the FCC’s insistence on a user opt-in.

157. While there is still some doubt, as a technical matter, it appears that the use of the Bluetooth overlap approach is more conducive to preservation of privacy than the GPS-based approach, Farr, *infra* note 161.

158. *Attorneys General Ask Apple and Google to Ensure All Contact Tracing Apps Serve a Public Health Purpose*, NAT’L ASS’N OF ATT’YS GEN., (June 16, 2020), <https://www.naag.org/naag/media/naag-news/attorneys-general-ask-apple-and-google-to-ensure-all-contact-tracing-apps-serve-a-public-health-purpose.php>. On June 16, 2020, the National Association of Attorneys General sent a letter to the chief executive officers of Google and Apple requesting them to require that all contact tracing and exposure notification apps be affiliated with a public health authority and removed from their respective marketplaces once the COVID-19 health crisis has ended.

measures. There is little reason for legal concern at this point if use of the app is strictly voluntary and the information regarding the contact with an infected person goes no further.

However, major privacy law and policy issues arise if (i) use of the technology is mandatory, (ii) information regarding a user's status, activities or whereabouts is shared with public health or law enforcement authorities, or (iii) any sort of action—such as home or other quarantine or activity restriction—is required of anyone in the process based upon information derived from the app. It cannot be denied that mandatory use is likely to be helpful to at least some extent in stopping virus spread, but making it mandatory substantially changes the privacy and civil liberties analysis. However, so long as use is voluntary, there is only so much value to public health authorities, who have a genuine need to fully understand and act upon virus status and spread.¹⁵⁹ The reference to 'practically useless' in the previously footnoted article makes the point.

To date, app use is purely voluntary in the US, and technology providers such as Apple and Google are resisting such sharing despite requests from state health authorities.

But as the tech giants have revealed more details, officials now say the software will be of little use. Due to strict rules imposed by the companies, the system will notify smartphone users if they've potentially come into contact with an infected person, but it won't share any data with health officials or reveal where those meetings took place.¹⁶⁰

While not necessarily representing a majority viewpoint, many civil liberties and privacy observers argue that a voluntary approach is essential. An observer from the Electronic Frontier Foundation explains: "'Having consent and good processes to grant and withdraw consent is critical,' said Bennett Cyphers, a staff technologist at EFF by phone."¹⁶¹ An article on a popular business site is aptly titled: *The Covid-19 response must balance civil liberties and public health—experts explain how.*¹⁶²

159. Reed Albergotti & Drew Harwell, *Apple and Google are building a virus-tracking system. Health Officials say it will be practically useless*, WASH. POST, (May 15, 2020), <https://www.washingtonpost.com/technology/2020/05/15/app-apple-google-virus/>.

160. *Id.* However, apparently countervailing concerns of state Attorneys General discussed *supra*. No response to such letter had been provided prior to this article going to press.

161. As a practical matter, users who do not consent can simply not have a smartphone at all or turn off their phones or their location services functions (or not carry them at all) to frustrate the system.

162. Christina Farr, *The COVID-19 response must balance civil liberties and public health—experts explain how*, CNBC, (Apr. 18, 2020), <https://nam02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.cnbc.com%2F2020%2F04%2F18%2F-covid-19-response-vs-civil-liberties-striking-the-right->

The recent adoption by New York and New Jersey of a voluntary Bluetooth-based app which is seen as less intrusive than any GPS-tracking-based app, may expedite adoption of technology based mitigation efforts.¹⁶³ The Bluetooth app simply indicates when someone using it has been within six feet of someone else who is using it and has tested positive. It does not create a record of where someone has been.

Once there is some mandatory element to use such apps or the information they provide, a number of social policy considerations must be taken into account. For example, if such measures can be used to provide public authorities with information about someone's activities and locations, it allows deduction of their political, social, and perhaps their sexual preferences in a manner which may chill activity and expression.

More fundamentally, if a person can be forced into quarantine because of data generated from such technology, this will impact many aspects of their life and livelihood. In the most sophisticated technology-based tracking program in use, that of Washington State, the contact tracers, who are in large part National Guard members, nominally do not have any formal authority to force anyone to do anything.

However, Washington's Governor, Jay Inslee did not rule out such a mandatory approach, saying merely that he hoped it would not be necessary.

Inslee said guardsmen serving as contact tracers will not have any law-enforcement powers. Asked what would happen to people who refuse to get tested or go into isolation, he said the state was getting a high percentage of compliance with current requirements. "It just shouldn't come to that," he said.¹⁶⁴

There is little doubt that a mandatory approach is seen by knowledgeable observers as more effective from a health standpoint:

balance.html&data=02%7C01%7Cmartin.robins%40fisher-broyles.com%7Cd047a7cf0e7b48cc157408d80a5498f7%7C9e8fa05ee48847f48de9cd9bd0adf758%7C0%7C0%7C637270705746827041&data=zbU0oRm%2FO9cHDSR%2BMdOtPz1Uha18WXDsQns8UNKfmTU%3D&reserved=0.

163. Will Feuer & Kif Leswing, *New York launches coronavirus contact tracing app as cases rise in hot spots*, CNBC (Oct. 1, 2020), <https://www.cnbc.com/2020/10/01/new-york-launches-coronavirus-contact-tracing-app-as-cases-rise-in-hot-spots.html>.

164. Jim Camden & Arielle Dreher, *Washington Ready to Launch Contact Tracing Program, Gov. Says*, GOV'T TECH., (May 13, 2020), <https://www.govtech.com/health/Washington-Ready-to-Launch-Contact-Tracing-Program-Gov-Says.html>.

University of Washington School of Law associate professor Ryan Calo, argues that we can go too far in preserving privacy above all other factors.

Calo looks at Google and Apple's Bluetooth approach and sees other problems. Because it's voluntary, that might provide people with a false sense of security if they don't get an alert. Those who have opted out might be walking around with Covid-19 and infecting others without ever being picked up with the system . . .

In Calo's view, contact tracing could be more effective if it wasn't voluntary, and closely linked with public health reporting.¹⁶⁵

C. *Non-US Mandatory Approach*

European public health authorities, operating under the GDPR, agree with the desirability of widespread adoption, but struggle with the strong bias of the GDPR against it. "Experts estimate that 60% of a country's population would need to use the app for it to be effective in preventing a second wave of infections."¹⁶⁶

Support for the efficacy of such a mandatory approach can be found in the experience of Taiwan, which by most accounts did an excellent job of combating the virus and keeping its consequences to a minimum. A fundamental—but far from the only—element of the Taiwanese strategy was the curtailment of privacy for the duration of the threat in the opposite manner of that contemplated by pending US legislation.

Despite its democratic credentials and open political culture, Taiwan unflinchingly curtailed privacy and individual liberty in the service of protecting public health during the COVID-19 epidemic. Individuals under isolation or quarantine orders—either because they returned from abroad or because they had contact with an infected person—had their

165. Farr, *supra* note 161.

166. Bojan Pancevski & Sam Schechner, *Coronavirus Contact—Tracing Apps Launch Across Europe Amid Hopes for Broad Adoption*, WALL ST. J., (June 16, 2020), https://www.wsj.com/articles/coronavirus-contact-tracing-apps-launch-across-europe-amid-hopes-for-broad-adoption-11592319612?emailToken=e91df4923699524fb76bfea008e66f24kmyF1kZ1uJbQTEXY3kqBN/CyU-CIhi-haZtX0Xj8f2y5X4rAXt+8dv+uPQZ6drnZwFjaW8MeGu26+y2JuatRiN6BLZVG6+XTCYRyxUCPkUuzodDXNhGFjE+DNLUIJVvphl0jOYjNwRvg3mZlx0XDo6rg%3D%3D&reflink=article_email_share (distinguishing between Bluetooth and GPS-based approaches in a privacy context).

cell phones tracked and were immediately accosted by police if they left their homes or turned off their phones.¹⁶⁷

D. Need for Unified Approach

To the extent that such mandatory approach is seen as a legitimate device for combating the virus, the authors favor a robust national debate balancing the detriment associated with abridgement of liberty with the undeniable benefit associated with reduction of serious disease. One can reasonably view the situation from several perspectives, but it is curious to have actual legislation such as the CCPA restricting collection and commercial use of information derived in this manner, at the same time that there is a good deal of interest in its deployment in situations where the consequences of its use are likely to be so much greater and subject to no such constraints. Mr. Snowden's concerns regarding use of personal information against citizens by military and law enforcement have extra meaning in this context.

Federal legislation introduced by two Democratic Senators and one Republican Senator to regulate such usage is currently pending.¹⁶⁸ For example, a Senate bill sponsored by Sens. Cantwell, Cassidy, and Klobuchar would require the same sort of opt-in.¹⁶⁹ The authors believe that some sort of federal¹⁷⁰ legislation of this nature is in order. In the meantime, the effort of New York authorities to subpoena contact information from attendees at a party, which

167. Steven Weber & Nils Gilman, *The Long Shadow of the Future*, NOEMA, (June 10, 2020), <https://www.noemamag.com/the-long-shadow-of-the-future/>.

168. Exposure Notification Privacy Act, S. 3861, 116th Cong. (2020).

169. Tony Room, *Members of congress to unveil bipartisan to regulate contact-tracing apps, fearing potential privacy abuses*, WASH. POST, (June 1, 2020), <https://www.washingtonpost.com/technology/2020/06/01/contact-tracing-congress-privacy/>; See also Krouse, *supra* note 2. Interestingly, this bill addresses both potential civil liberties concerns and concerns with commercial use of information gleaned from such app. A similar bill has been introduced by Senate Republicans. Alysa Zeltzer Hutnik & Lauren Myers, *Senate Republicans Release COVID-19 Privacy Bill*, KELLEY DRYE, (May 7, 2020), <https://www.adlawaccess.com/2020/05/articles/senate-covid-19-privacy-bill/>. The bipartisan bill “makes participation in commercial online exposure notification systems voluntary and gives consumers strong controls over their personal data, limits the types of data that can be collected and how it can be used, and contains strong enforcement provisions.” *Cantwell, Cassidy, and Klobuchar Introduce Bipartisan Legislation to Protect Consumer Privacy Promote Public Health for COVID-19 Exposure Notification Apps*, SENATE.GOV, (June 1, 2020), <https://www.commerce.senate.gov/2020/6/cantwell-cassidy-and-klobuchar-introduce-bipartisan-legislation-to-protect-consumer-privacy-promote-public-health-for-covid-19-exposure-notification-apps>.

170. As opposed to state legislation, with respect to which conflicting and differing obligations, and likely tied to different technologies, would likely make unwieldy even the most well-conceived program.

apparently contributed to the spread of COVID-19, indicates the likely direction of a mandatory approach.¹⁷¹

Reasonable minds can differ as to the manner and extent to which technology should be used to combat COVID-19, and other equally serious maladies, and the acceptable tradeoffs between such efforts at disease control and individual privacy and liberty. Public health authorities would be derelict in their responsibilities if they did not seriously explore all options for disease containment. However, the authors believe that in connection with such exploration, policy-makers must acknowledge that such tradeoffs are an important reality and take them into account when determining the balance which best serves society.

XII. CONCLUSION

In a complex, technologically-based society, where harm can befall individuals in several ways if their sensitive information falls into the wrong hands, it is essential that there be meaningful regulation of the manner in which personal information is collected, stored, transmitted, and utilized. However, the various considerations implicated by such efforts to avoid harm make it essential that discussion focus on the specific harms which are deemed to be of greatest importance so that the proper, least burdensome remedial measures can be prescribed. The medical, economic, and social consequences of COVID-19 and governmental responses to it, which implicate many of the considerations discussed in this article, add a major new dimension to the analysis. The authors hope that this article will play a small role in helping policy-makers address both existing and proposed new laws to identify the various concerns and related consequences.

171. Peter Sullivan, *New York county issues subpoenas to people refusing to talk to contact tracers*, THE HILL, (June 1, 2020), <https://thehill.com/policy/healthcare/505437-new-york-county-issues-subpoenas-to-people-refusing-to-talk-to-contact>.

APPENDIX

PRIVACY POLICY EXCERPTS¹⁷²

(OUTLINE LETTERING ADDED BY AUTHORS)

XYZ Shirt Warehouse, Inc. (“XYZ”) collects customer information to facilitate and enhance your shopping experience. This privacy policy (“Policy”) is intended to assist you in understanding what information we gather about you when you visit one of our stores or our websites, how we use and share that information, and the safeguards we have in place for that information. This Policy applies to the information collected at any of our stores, on the phone, and through our websites that link to this Policy. References to XYZ.com shall refer generally to all of XYZ’s online services, including mobile applications. In this Policy, “we” and “our” mean XYZ, and “you” means any person who visits our website, uses our mobile application, or visits our U.S. stores.

A. Information We Collect and How We Use It

“Personal information” means information that identifies, relates to, or describes, directly or indirectly, a particular individual, such as: name, address, email address, or phone number.

We collect the following categories of personal information through XYZ.com, our stores, customer service and otherwise, and use it for typical business management, operational and commercial purposes (including to defend and protect us and others from harm or legal claims, and as required by applicable law) and as described more specifically below:

- Personal identifiers. We receive personal identifiers (such as your name, phone number, email address, billing address, shipping address, password, device ids, and IP address), personal identifiers of others (such as an order recipient’s name and address) and use them to respond to requests, fulfill and deliver orders for merchandise and services, process returns or exchanges, contact you or others about an order or delivery, facilitate surveys, promotions, sweepstakes, and contests, manage accounts and preferences, facilitate rewards programs and accounts and to communicate with you for marketing and informational purposes.

172. Included in a policy circulated via email to customers and posted January 8, 2020. The company circulating such policy in response to the CCPA effectiveness has both physical store and online e-capability. This example was chosen because it reflects consideration of most of the issues discussed in the text with respect to the CCPA, with the notable exception of the household concept.

We will also create a client number when you make a purchase and a XYZ VIP Rewards Number when you sign up to be a member so we can identify you. We may also receive your driver's license number when you make product returns, which we use for fraud prevention and to meet legal obligations.

- Message and product review content. We collect the messages you submit through contact, sign-up, surveys, purchase and product review forms on XYZ.com, such as customer service requests, messages to delivery recipients and delivery instructions. We use this information to respond to and fulfill your requests, better understand your needs and preferences, enhance and personalize our product offerings to you and improve XYZ.com and our service and merchandise offerings.
- Audio and visual information. We receive any digital photos you submit through XYZ.com and post this information to public areas of XYZ.com at your direction. To help protect you and others, we monitor and record video and take photographs of the public areas of stores for security, fraud, loss prevention, incident reporting and other operational purposes. We may record customer service telephone calls for quality purposes and to meet our legal obligations.
- Financial information. We receive financial information (such as payment card and bank account information) to process payments for merchandise and services you purchase on XYZ.com.
- Commercial transaction information. We collect and generate commercial transaction information (such as records of merchandise and services purchased) when you make purchases on XYZ.com and in stores and when you make purchases using the XYZ-branded payment card. We use this information to deliver and fulfill your orders, process your returns or exchanges, improve our service and merchandise offerings, tailor our marketing efforts and administer accounts, and for internal operations and reporting purposes.
- Personal characteristics. We receive personal characteristics (such as your birth date and birth dates of others, footwear size information, and locale) when you provide the information to us. We use the birth date information to personalize offers and gifts. We use footwear size information to provide you with the products you order and save your preferences. We collect location when you submit reviews, so we can personalize the reviews for others.

B.

- Geo-Location Information. We collect mobile device identifiers and geo-location information of visitors' devices in and around our stores to monitor foot traffic to help us understand how shoppers move around our stores, identify what shoppers seem interested in and improve the shopping experience.
- Inferences from the information listed above. XYZ will use the information listed above to draw inferences about your preferences (such as your preferred brands and styles) to help us provide you with personalized content and offers and help us develop and provide better merchandise and services.

C.

In addition, we and our third-party partners, such as advertising networks, social media widgets, and analytics providers, may automatically collect other categories of personal information using cookies and similar technology when you use XYZ.com, our emails, and in-store wi-fi services available near or in our stores. We use this information to provide and improve our website and order processing, for anti-fraud purposes, to tailor your experience on XYZ.com and our marketing efforts, to provide our in-store wi-fi services and to create aggregate internal reports on website usage and activity, such as views of certain merchandise. These additional categories may consist of:

- Online identifiers. XYZ may collect your IP address and other device and online identifiers when you use XYZ.com.
- Geo-Location Information. Many mobile devices permit applications to access real-time geo-location information. We also may collect and use such information, with your consent. In addition, some of the information we collect, such as IP addresses, may be used to estimate an approximate location of the device you are using to access XYZ.com. We use location information to enhance and personalize the features and functionality of XYZ.com and merchandise and service offerings.
- Website activity information. XYZ may monitor and collect XYZ website activity information and device information, such as website clicks, content and page views, the website each visitor visited prior to our website, domain type, browser version, and internet service provider.

- Inferences from the information listed above. XYZ will use the information listed above to draw inferences about your shopping preferences (such as your preferred brands and styles) to help us provide you with personalized content and offers and help us develop and provide better merchandise and services.

XYZ collects various types of personal information from and about California residents both online (at XYZ.com) and offline during the course of our customer relationship.

D. Sharing for Others' Marketing Purposes.

Under California law, if you are a resident of California, you may make a written request to XYZ to request how we have shared your information with third parties for their direct marketing purposes. In response to your written request, XYZ is allowed to provide you with a notice describing the cost-free means to opt-out of our sharing your information with third parties with whom we do not share the same brand name, if the third party will use it for their direct marketing purposes.

XYZ has chosen to provide you with a cost-free means to opt-out of such sharing. If you would like to instruct us to no longer share your personal information with third parties who will use it for direct marketing purposes, please let us know by contacting us at customerservice@XYZ.com or at the following address:

POSTAL ADDRESS:

If you have any questions about this opt-out procedure, please write to the address provided above.

E. Online Tracking.

XYZ may permit third parties to track the individual visitors to its website and the activities of those visitors on XYZ.com over time, and they may track those visitors across other websites and online services, if those websites and apps also use the same partners (as described above in the "Cookies, Pixel Tags, and Similar Technology" section). Currently, XYZ does not offer the option for its website visitors to make a "Do Not Track" election and does not have the capability to respond to electronic "Do Not Track" signals. XYZ reserves the right to add such capability to its website at any time in the future and will notify website visitors of this change in capability through an update to this Policy.

F. Privacy Rights Requests.

California consumers have the right to request:

- the deletion of the personal information we have about them;
- additional information about whether and how we have collected, used, disclosed and sold personal information about them;
- the specific pieces of personal information we have about them; and
- an opt-out of future sales of their personal information at xyz.com/opt-out.

California consumers also have the right not to receive discriminatory treatment if they exercise the rights list above.

When you make a request, we may require that you provide information and follow procedures so that we can verify the request and your jurisdiction before responding to it. The verification steps we take may differ depending on the request you make. We will match the information that you provide in your request to information we already have on file to verify your identity. If we are able to verify your request, we will process it. If we cannot verify your request, we may ask you for additional information to help us verify your request.

To make requests, California consumers may call us at 1-866-379-7463 or contact us through the web page located here. Consumers will be required to submit their name, email address, and telephone number, and may also be asked to provide their address, XYZ VIP Rewards Number, and a recent order number so that we can verify the request. Please provide as much of the requested information as possible to help us verify the request. We will only use the information received in a request for the purposes of responding to the request.

California law permits California consumers to use an authorized agent to make privacy rights requests. We require the authorized agent to provide us with proof of the California consumer's written permission (for example, a power of attorney) that shows the authorized agent has the authority to submit a request for the California consumer. An authorized agency must follow the process described above to make a request, and we will additionally require the authorized agent to verify his/her own identity and we may confirm the agent's authority with the California consumer about whom the request was made.

G.

We do not sell personal information for money; however, in the prior 12 months, we have permitted third parties (online analytics and advertising

companies, affiliates, and co-brand partners) to use personal information for their business and commercial purposes that may not directly benefit XYZ (such as to provide and improve their products and services or for their or others' marketing purposes). This sharing may be considered a "sale" of personal information under the California Consumer Privacy Act. We shared (or "sold") for these purposes the following categories of personal information: personal identifiers (including device identifiers), ratings and review content, commercial transaction information, personal characteristics, XYZ.com browsing activities, and inferences drawn from these categories. We do not knowingly "sell" the personal information of individuals under the age of 16. You may access our page to opt out of future "sales" [at this link]. If you opt out, we may ask you to consent to such "sales" in the future.

H.

We employ reasonable security measures to secure the information we receive. For example, we take the following types of security measures: use of technologies and policies such as limited access data-centers, firewall technology, and secure socket layer certificate authentication. Any credit card/debit card information will be encrypted by the use of a "token" for security purposes.

We designed xyz.com to accept orders only from Web browsers that accept cookies and permit communication through Secure Socket Layer (SSL) technology. SSL is encryption technology that provides security while information is being transmitted over the Internet.

While we implement the above security measures on this website, you should be aware that 100% security is not always possible.

We encourage you to take steps to help protect the confidentiality and security of your xyz.com account and personal information by periodically reviewing your xyz.com account and immediately reporting any unexpected activity or unrecognized information; installing the latest security updates and anti-virus software on your computer to help prevent malware and viruses; using complex and diverse passwords; keeping your password private; password protecting your computer and mobile device; and signing out of your xyz.com account before closing your internet browser.

I. Merger, sale, or other asset transfers.

In the event of a merger, acquisition, financing due diligence, reorganization, bankruptcy, receivership, sale of company assets, or transition of service to another business unit (whether by private sale, through operation of law, as part of a divestiture plan, or otherwise), we will provide any personal information and transaction history associated with each such business unit to the

persons and/or entities assuming control of such business unit and our advisors or as otherwise necessary to complete the transaction as permitted by law or contract.