CONSUMER AND CHILD DIGITAL PRIVACY: ISSUES AND RECOMMENDATIONS FOR STATE LEGISLATION

REPORT FOR THE

THE AD HOC SUBCOMMITTEE ON CONSUMER PRIVACY OF THE MARYLAND CYBERSECURITY COUNCIL

DECEMBER 19, 2022

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report is a staff work product for the Maryland Cybersecurity Council's Ad Hoc Subcommittee on Consumer Privacy.[1] The report offers context and recommendations related to the digital privacy of Maryland consumers in general and children in particular. As a staff product, it stands next to the comments and presentations of stakeholders and subject matter experts solicited by the Subcommittee and provided over four open meetings this year.[2] By design[3], this report, and the convening work of the Subcommittee, were intended to create a record to inform discussions about digital privacy legislation for the State.

Consumers face enormous privacy challenges. Sensitive data about them is collected in innumerable ways, associated with them, categorized, and shared widely across the consumer data ecosystem. In a wired society, it is impossible to avoid this. Further, privacy policies do not easily enable consumers to understand how their data is collected and used and provide few tools they can use to control collection and use. Finally, the risks to consumers posed by data collection and use are reaching a critical stage with the expanding commercial interest in biometric information.

This is not to say that all data collection and use is without benefit—consumers using online banking, for example, benefit from fraud detection technology working in the background. As one White House report has noted, "[m]uch of this innovation is enabled by novel uses of personal information."[4] But the same report points out that a lack of consumer trust can be a barrier to innovation. "Privacy protections are critical to maintaining consumer trust in networked technologies."[5] This is not theoretical. In a 2019 Pew poll, 52% of adults surveyed indicated "that they decided not to use a product or

---

[1] This report was drafted by Dr. Greg von Lehmen, University of Maryland Global Campus, as assigned staff to the Maryland Cybersecurity Council. Appendix A was contributed by Quinn Laking and Nikita Vozenilek, two third-year law students at the University of Maryland School of Law. The opportunity to ask follow-up questions of outside presenters to the subcommittee on other aspects of the law likewise contributed to the report. Helpful to the report's technical aspects was the review by Joseph Carrigan, Senior Security Engineer at Johns Hopkins Institute for Assured Autonomy. Markus Rasuchecker, subcommittee member, and Howard Barr, Assistant Attorney General and Principal Counsel, Maryland Department of Information Technology, made suggestions that improved the report's writing. Subject to final, minor editing, the report was adopted by the subcommittee at its December 13, 2022, meeting for inclusion in the record to help inform digital privacy legislation for the State of Maryland. (See "Subcommittee Meetings" at https://www.umgc.edu/administration/leadership-and-governance/boards-and-committees/maryland-cybersecurity-council)

[2] The recordings and other materials are available for each meeting: August 23, 2022 (https://www.umgc.edu/content/dam/umgc/documents/upload/8232022-recording-meeting-consumer-privacy.pdf), September 22, 2022 (https://www.umgc.edu/content/dam/umgc/documents/upload/recording-of-the-meeting-on-september-22-2022.pdf), October 20, 2022 (https://www.umgc.edu/content/dam/umgc/documents/upload/recording-of-the-meeting-on-october-20-2022-ahccp.pdf), and November 18, 2022 (https://www.umgc.edu/content/dam/umgc/documents/upload/draft-minutes-for-november-18-2022.pdf).

[3] See opening charge of the Subcommittee Chair, Senator Susan Lee, at the August 23, 2022, meeting referenced above.

[4] The White House (2012). Consumer Data Privacy in a networked world: A framework for protecting privacy and promoting innovation in a global digital economy." See introductory letter. https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf

[5] Ibid.

service because they were worried about how much personal information would be collected about them."[6]

The concerns of consumers can be reformulated as a problem of cybersecurity risk management. Just as the case with enterprises, consumers wrestle with cybersecurity risk every day as regards themselves and their children. Overtime, states have helped consumers and parents manage this risk by giving them tools to manage their exposure. All states, for example, have data breach notification laws to alert consumers to take protective action. Some states require credit reporting agencies to allow consumers to freeze their credit reports for free.

But the tools and other protections should pace with advances in technology and what is known about the related risks. As mentioned below, various states have done this by enacting laws that in addressing cybersecurity risk to consumers, enable them to better manage the risk to themselves and their children. Arguably, the more agency consumers feel with respect to the collection and use of their personal data, the more trust they will likely have.

Recommended are certain foundational principles for affording greater protection of Maryland consumer privacy in a digital world and contributing to a relationship of trust between consumers and companies that collect and use their data. At the front end, these principles provide for:

- Greater consumer awareness of who holds their data, including not only companies with which they have a consensual relationship but also data brokers. Recommended is a State registration requirement for data brokers as implemented in Vermont and other states.
- Greater consumer control over what data is collected by companies with which they interact and how it is used, including the option to opt-out of data sharing or selling to third parties
- Transparent and understandable privacy policies to enable consumers to easily exercise these choices
- Data collection, use, and retention that is consistent with the consumer's relationship with the company and what is needed to provide services to the consumer.

With respect to data held by companies:

- Consumers should have access to the data companies hold on them in a format that the consumer can understand (data portability)
- Consumers should have the right of rectification or the right to correct information that is in error
- Subject to certain legal restrictions, consumers should be able to delete all of their data held by a company, including all data compiled by the company regardless of

[6] Auxier, B and Raine, L. (2019, November 15). Key takeaways on Americans' views about privacy, surveillance, and data-sharing. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/

source, and that the deletion should extend to third-party recipients of the consumer's data
- Companies should be required to have data security practices reasonably commensurate with the sensitivity of the data held.

With respect to enforcement:
- Accountability through appropriate mechanisms and penalties to ensure that the principles are observed.

These principles do not relieve all challenges confronting the consumer, such as the multiplicity of privacy policies and the lack of a true global data deletion option that would remove sensitive consumer data throughout the consumer data ecosystem. But recognizing these limitations, the principles can improve the consumer's position vis-à-vis the collection and use of their data. Furthermore, the implementation of these principles in some form is not impractical. Public concern is driving momentum among governing bodies to implement these principles in some measure. This is true not only for EU citizens under the General Data Protection Regulation (GDPR) but also now for consumers in five states, including California, Colorado, Utah, Virginia, and most recently, Connecticut. Finally, this means that many companies, certainly the largest ones, and the one collecting and using the most data, are already implementing them for specific populations. Codifying these principles in Maryland would extend them to Maryland residents.

While the consumer privacy principles discussed above are applicable to data collected on children, there are issues specific to children that this report discusses. The governing federal statute pertaining to the activity of children online and the related responsibilities of companies is the Children Online Privacy Protection Act (COPPA). While a crucial step forward in in protecting children online, there have been calls to strengthen the regulatory framework in the light of issues that experience has brought to light. As is the case with general consumer protection, the likelihood that these issues will be addressed at the federal level are difficult to assess but can and are being addressed at the state level.

With respect to the collection and use of children's digital data, the report makes the following recommendations for Maryland:

- Require constructive knowledge in lieu of actual knowledge as the standard against which general audience apps and other platforms are held to determine whether they must comply with children's online protections. As a general matter, constructive knowledge would mean that given the data practices of an "operator" as defined by COPPA, it would be reasonable to assume that the operator knew or should have known children are using their platform
- Engage with Apple and Google about expanding the scope of efforts to minimize child-directed in their stores that are not COPPA compliant.

- Ban targeted advertising on child-directed apps**.** This recommendation aims to address the harms to children from targeted advertising that have been identified in subcommittee testimony.[7]
- Require data minimization with respect to data collected on children. Data minimization is a general privacy recommendation of the Federal Trade Commission[8] and is advocated as a practice with respect to children's data.[9] It would require operators to limit data collection to what is reasonably necessary to provide a product or service, to be transparent about the specific purpose of the data collection no later than the time of collection, and to retain data only for the period of time necessary to process a transaction or to provide a service.
- Rectification and deletion rights**.** Already a right for consumers in general in five states, this recommendation would specifically extend these rights to children's data in Maryland.
- Security. Similarly, consistent with consumer privacy principles and legislation in other states, mandate security standards for data collected and transmitted on children that are reasonably commensurate with the sensitivity of the data.

[7]Hinkle, H. (2022, August 23). Testimony before the Ad Hoc Subcommittee on Consumer Privacy, Maryland Cybersecurity Council, p.5. https://1drv.ms/b/s!AjqEqIxJkAfagdd7GY7Tt37azAatJQ?e=BO3kbv and Ly, I (2022, August 23). Testimony before the Ad Hoc Committee on Consumer Privacy. https://1drv.ms/b/s!AjqEqIxJkAfagddBIdWyGonkdklDEQ?e=VkSy2F

[8] Federal Trade Commission (2015, January). Internet of things: privacy in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[9] See for example, Ly, idem.

ORGANIZATION OF THE REPORT

Given the complexity of the issues, the report discusses general consumer privacy and child privacy separately. Each section provides context, identifies key issues, and offers recommendations for addressing those issues. Appendix A provides an in-depth analysis of state and federal efforts relating to these issues.

Section I: Digital Consumer Privacy in General

Understanding consumers in granular ways and predicting their behavior has become a core industry in every mature market economy. As a development, it is responsive to the intrinsic market incentives to be sell more products and services, to innovate, and to maximize return. Various developments have enabled the compilation and purposing of data on individuals. These include computers and software, the digitization of information, the internet and the technology that connects to it, the low cost of data storage, and the availability of new tools, principally big data analytics, machine learning, and artificial intelligence.

Ubiquitous data collection

The data collected today on consumers is marked by its volume, variety, and velocity, i.e., its continuous and real-time character.[10] These consumer profiles are built from several data sources. Online presence is the most extensive one.

Consumer data is captured by internet service providers (ISPs), and the various applications that ride on their service (e.g., search engines, social media platforms, other websites, games, streaming TV). Some of this data is consciously provided by the consumer, such as information required to process transactions or added to social media platforms. Much is collected passively, including IP address, browsing history, time on page, and associated details about the computer device being used, including the unique device identifier, settings, and plugins.[11] At any one time, browsing activity is captured by many different tracking companies.[12]

Applications on mobile devices and internet of things devices provides other sources of data. Applications on mobile devices collect a variety of information that may be related to the service, like precise geolocation, and other information that may be completely unnecessary,

---

[10] The White House (2014, May). Big data: Seizing opportunity, preserving values. https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf

[11] For a technical discussion of data captured and transmitted to backend servers, see Leith, D (2021, March 10). Web browser privacy: What do browsers say when they phone home? IEEE. https://ieeexplore.ieee.org/document/9374407 . The key conclusion: "Overall, we find that both the desktop and mobile versions of Brave do not use any identifiers allowing tracking of IP address over time, and do not share details of web pages visited with backend servers. In contrast, Chrome, Firefox, Safari, and Edge all share details of web pages visited with backend servers. Additionally, Chrome, Firefox and Edge all share long-lived identifiers that can be used to link connections together and so potentially allow tracking over time. In the case of Edge these are device and hardware identifiers that are hard/impossible for users to change. On mobile devices, but not desktop devices, Firefox also shares device identifiers." Page 41615

[12] For example, see the findings of a 2018 study at https://whotracks.me/

such contacts and photos on the mobile device.[13] Wearables collect and transmit exercise or other health data to companies providing the product. A variety of other internet of things (IoT) devices that permit voice activation of services, vacuum the home, and provide home security, etc., all collect and store data.

> Prior to the applications themselves, it has been shown that the two principal operating systems—iOS and Android—transmit data to Apple and Google that provides a rich source of information to those companies about the consumer. At start-up, this includes unique and persistent device identifiers and the information about the telecommunication provider. Applications never used, like iCloud on the Apple or Chrome or the YouTube app on the Android, also periodically call back to Apple and Google servers. Finally, data collection continues even when a) the most conservative privacy settings are selected—turning off geolocation, the analytics and improvement option on iOS, and the usage and diagnostics option on Google—and b) the device is not in use.[14]

Telemetry in itself is not necessarily a privacy intrusion, since it may serve purposes related to software or device maintenance and service.[15] However, it does become a matter of concern "when data can be tied to a specific user, especially over extended duration and old/new device pairs" [16] and can be used for other purposes.

> The collection of so much data by Apple and Google raises at least two major concerns. Firstly, this device data can be fairly readily linked to other data sources, e.g., once a user logs in (as they must to use the pre-installed app store) then this device data gets linked to their personal details (name, email, credit card etc.) and so potentially to other devices owned the user, shopping purchases, web browsing history and so on. This is not a hypothetical concern since both Apple and Google operate payment services, supply popular web browsers and benefit commercially from advertising. Secondly, every time a handset connects with a back-end server [even with the geolocation off] it necessarily reveals the handset IP address, which is a rough proxy for location. The high frequency of network connections made by both iOS and Google Android (on average every 4.5 minutes) therefore potentially allow tracking by Apple and Google of device location over time.[17]

---

[13] Kelly, H (2021, July 15). Lots of apps use your personal contacts. Few will tell you what they do with them. Washington Post. https://www.washingtonpost.com/technology/2021/07/15/contacts-sharing-privacy/ and Cohen, J. (2022, January 11). These Apps Collect the Most Personal Data. PC Mag. https://www.pcmag.com/news/sick-of-data-collection-try-these-apps-instead

[14] Leith, D (2021, March 25). Mobile Handset Privacy: Measuring The Data iOS and Android Send to Apple And Google. In Security and Privacy in Communication Networks, 17th EAI International Conference, SecureComm 2021, Virtual Event, September 6–9, 2021, Proceedings, Part II. Page, 2 https://www.scss.tcd.ie/doug.leith/apple_google.pdf

[15] See industry comments in Spring, T. (2021, March 31). Apple, Google both track mobile telemetry data, despite users opting out. Threatpost. https://threatpost.com/google-apple-track-mobile-opting-out/165147/

[16] Leith, idem, page 3.

[17] Idem, page 2. Insert added to the quote.

Consumer profiles are enriched through merger and acquisitions which enable companies to bring together consumer data held by other providers. For example, in a study of the six major telecommunications/internet service providers, the Federal Trade Commission (FTC) noted that:

The vertical integration of ISP services with other services like home security and automation, video streaming, content creation, advertising, email, search, wearables, and connected cars permits not only the collection of large volumes of data, but also the collection of highly-granular data about individual subscribers. As noted above, a sizable number of the ISPs in our study combine their customers' information across product lines. This means a single ISP has the ability to track the websites their subscribers visit, the shows they watch, the apps they use, their energy habits, their real-time whereabouts and historical location, the search queries they make, and the contents of their email communications.[18]

As a more recent development, retailers have begun to collect biometric information both online and in-store. Some retailer websites capture biometric information of consumers purchasing certain products like glasses and makeup.[19] Others record shoppers in stores as they shop or checkout and in some cases use facial recognition technology to identify potential shoplifters.[20] Security companies use digital biometric information (face, fingerprints) to offer facility access control and other identity confirmation purposes.[21] A number of class action suits have been settled against large social media platforms alleging that without consumer consent they scanned, stored, and in some cases sold scans of biometric information such as photos to third parties.[22]

Finally, information resellers or data brokers are major compilers and sellers of consumer data. These companies start with name, address, contact information and add other data like education, employment, ethnicity, purchase history, sexual orientation, political orientation, religious affiliation, credit history, hobbies, income, whether married, divorced, or convicted of a crime, among many other data points)[23]. These data are dynamically refreshed and include timely and

[18] Federal Trade Commission (2021, October 21). A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers. Pages 110-111. See in this connection the Executive Summary and also Attachment B of the report that illustrates the depth of data collection. https://www.ftc.gov/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers

[19] James, D (2022, November 2). Retailers are wading deeper into customer data. States are raising the alarm. https://www.retaildive.com/news/walmart-peloton-snap-biometric-customer-data-consumer-privacy-laws/634746/

[20] Insider Intelligence (2019, October 3). How retailers are using biometrics to identify consumers and shoplifters. https://www.insiderintelligence.com/content/how-retailers-are-using-biometrics-to-identify-consumers-and-shoplifters

[21] Doffman, Z (2019, August 14). New data breach has exposed millions of fingerprint and facial recognition records: Report. https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=620f862446c6

[22] NBC Chicago (2022, August 24). Here's a look at settlements stemming from Illinois' Biometric Privacy Act. https://www.nbcchicago.com/news/local/heres-a-look-at-all-the-settlements-stemming-from-illinois-biometric-privacy-act/2922736/

[23] Beckett, L. (2014, June 13). Everything we know about what data brokers know about you. Pro Publica. https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you. See also Kroft, S. (2014, March 9). The data brokers: Selling your personal information. https://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/ To enable interoperability of data within the data ecosystem, the Interactive Advertising Bureau (IAB), an industry group, has devised an audience taxonomy that indicates how

actionable information, such as whether a consumer is expecting a child. Data brokers acquire their data from public records, publicly available information on social media, through blogs, corporate announcements, and other sources, and from nonpublic information that the companies collect themselves, obtain from affiliates, or purchase from other companies.[24]

While this data and its supporting infrastructure have given rise to reference services and various risk mitigation products aimed at business[25], the principal driver for compiling detailed individual consumer profiles is digital advertising. Digital advertising in the US reached $211 billion in 2021 and has been predicted to approach $240 billion in 2022.[26] Google, Amazon, and Facebook and their ad tech arms account for more than 60% of this spend.[27] The large proportion of this spend is on "programmatic advertising", which includes real time bidding (RTB)[28].

RTB is an essential part of data flows across the consumer data ecosystem. In RTB, advertising is targeted at a particular consumer while she is online. The advertising is based on her individual behavioral data and in a common scenario is sold to the highest bidder in the milliseconds between clicking on a website and the website's loading.[29] The "bidstream" data, which may be provided on a bid exchange to hundreds of participating companies, is attached to a unique consumer ID and enables targeting by variables such as geographical location and consumer classification, e.g., LGTB+, substance abuse, depression, infertility, and brain tumor.[30] The bidding is automated, conducted by algorithms that make decisions to bid or not based on the bidstream data. The scale of these consumer data flows is captured by Statista. In 2021, bidstream data was put on an exchange 810 times per day per person in Maryland.[31] Note that

---

many variables data is collected on. See the IAB Lab audience taxonomy at https://iabtechlab.com/standards/audience-taxonomy/

[24] Cackley, A. (2019, June 11). Consumer privacy: Changes to legal framework needed to address gaps. Government Accounting Office. GAO-19-621T. Pages 1 – 2. https://www.gao.gov/products/gao-19-621t See also Knowledge at Wharton (2019, October 28). Your data is shared and sold… What's being done about it? https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ Note that categories are blurred in that large tech companies, while registered as data brokers, hold vast troves of data and purpose this data through their own ad tech firms.

[25] Cackley, idem.

[26] Insider Intelligence (2022, April 20). Digital advertising in 2022: Market trends & predictions. https://www.insiderintelligence.com/insights/digital-advertising-market-trends-predictions/

[27] Lebow, S. (2021, November 3). Google, Facebook, and Amazon to account for 64% of US digital ad spending this year. https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending

[28] Amazon. What is RTB? Real time bidding explained. https://advertising.amazon.com/library/guides/real-time-bidding

[29] Clearcode (2021, July 20). How does real-time bidding (RTB) work? https://clearcode.cc/blog/real-time-bidding/. For an academic discussion, see Sayedi, Amin (2017, February 14). Real-time bidding in online display advertising. SSRN: https://ssrn.com/abstract=2916875

[30] Ryan, J (2020, September 21). Submission to the Irish Data Protection Commission. https://www.politico.eu/wp-content/uploads/2020/09/JohnnyRyanDocumnet.pdf For a discussion of this report in context, see Lomas, N (2019, May 20). GDPR ad tech complaints keep stacking up in Europe. Tech Crunch. https://techcrunch.com/2019/05/20/gdpr-adtech-complaints-keep-stacking-up-in-europe/ and the author's 2021 update at https://techcrunch.com/2020/09/21/irelands-data-watchdog-slammed-for-letting-adtech-carry-on-biggest-breach-of-all-time/

[31] Statista. Number of real-time bidding (RTB) U.S. consumer data transfers per person per day worldwide in 2021, by state of origin. https://www.statista.com/statistics/1327271/rtb-transfers-us-consumer-data-state/

the use of a unique identifier does not necessarily preclude the identification of individuals associated with that identifier.[32] With respect to "ad IDs", the Electronic Frontier Foundation has observed that [t]here is an entire industry of "identity resolution" companies that can readily link ad IDs to real people at scale"[33].

At some level, consumers have a sense that their activities are tracked and that detailed information about them is compiled and shared. In a 2019 poll[34], Pew found that:

- 71% of Americans "are at least somewhat concerned" about how much data is collected on them
- 62% "believe that it is not possible to go through daily life without having their data collected by companies"
- 59% say that they "understand very little or nothing" about what companies do with their personal data
- 81 % say "that the potential risks outweigh the benefits" when it comes to company-collected data"
- 70% feel that their data is "less secure than it was five years ago"
- 75% "say that there should be more regulation of what companies do with their data"

These poll findings frame the policy issues with respect to consumer privacy.

Six Significant Issues

1. **Privacy policies are broken.** As the vehicle for informing consumers about data collection and use, commercial privacy policies have come under criticism.[35] One legal scholar has noted that "privacy policies "are confusing, inconspicuous, long, and difficult to understand" and that "even experts find them misleading".[36] Similarly, a recent study conducted by faculty at Carnegie Mellon University and University of Michigan examined the privacy policies of 150 websites of various levels of popularity accessed by US consumers. Among their findings about the privacy choice section of these policies, the researchers noted that there was no dominant wording for headings, that there was missing, misleading, or unhelpful information, that targeted

[32] Lomas, N (2019, July 24). Researchers spotlight the 'lie' of anonymous data. TechCrunch. https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ See also Leith, D., idem, page 41617.

[33] Gebhardt, G. and Cyphers, B. (2021, July 13). Data brokers are the problem. https://www.eff.org/deeplinks/2021/07/data-brokers-are-problem

[34] Auxier, B and Raine, L. (2019, November 15). Key takeaways on Americans' views about privacy, surveillance, and data-sharing. Pew Research Center. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/ and the full report by Auxier, B., Rainie, L.., et al (2019, November 15) Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ For similar consumer concerns about health data in particular, see American Medical Association (2022). Patient perspectives around data privacy. https://www.ama-assn.org/system/files/ama-patient-data-privacy-survey-results.pdf

[35] Kumar, V and Iyengar, R, et al. (2020,). Finding a choice in a haystack: Automatic extraction of opt-out statements from privacy policy Text. Page 1. ACM https://usableprivacy.org/static/files/kumar_iyengar_www_2020.pdf

[36] Waldman, A (2018). A Statistical Analysis of Privacy Policy Design. Notre Dame Law Online. (Vol 93 Issue 1). Page 160. https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1050&context=ndlr_online

marketing opt-outs were ambiguous, and that privacy choice text had poor readability. Regarding the last, the study assessed that the privacy text did not meet the GDPR "clear and plain language" requirement as one metric.[37]

Other large surveys of consumer privacy policies have documented similar aspects of these policies. It has been observed, for example, that few policies are definitive about the third-parties with whom companies share data. Consequently, "[u]sers who read website privacy policies are therefore very unlikely to be notified of the parties which collect their data.[38] This despite the fact that the "level of information and the amount of data being collected and shared with third parties is massive."[39]

Of course, these challenges are multiplied by the number of privacy policies with which a consumer is confronted. Consumers have ongoing relationships across many companies, each of which collects, uses, and shares consumer data. The companies with which consumers interact include not only Fortune 500 companies that are established storefronts but the many providers whose apps consumers use for their specific utility. Further, the number of applicable policies is compounded where companies refer the consumer to the privacy policies of other companies with which they share data.

2. Generally, privacy policies offer Maryland consumers few tools to manage the collection and use of their personal information. A study that examined more than 6,800 US websites stratified by popularity found that the most prominent opt-out concerned marketing (60% of all opt-outs found) with only 17% of the opt-outs related to cookie tracking, only about 7% to third-party data sharing, and about 6% to opting out of analytics."[40] Another study found that "Do Not Track" (DNT) browser setting is rarely mentioned in privacy policies, and when it is, it is usually to specify that the expressed user choice is ignored.[41]

With respect to deletion rights, the aforementioned study of 150 websites found that about half allowed some data to be deleted, about a third offered the option of deleting the permanent account, and of these most did not identify a time frame for permanent deletion.[42] Another study mentions the service, JustDelete.me, that "provides a database with ratings of the ease of deleting data from over 500 different websites, and compiles direct links to the deletion options on those sites". The study notes that "nearly 40% of the websites listed in the database are rated as having

[37] Habib, H. et al (2020, August 1). An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS 2020) 387-406. Available at https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-hana_habib.pdf See also Waldman, A (2018). A Statistical Analysis of Privacy Policy Design. Notre Dame Law Online. (Vol 93 Issue 1). https://scholarship.law.nd.edu/cgi/viewcontent.cgi?article=1050&context=ndlr_online

[38] Libert, T (2018). An Automated Approach to Auditing Disclosure of Third-Party Data Collection in Website Privacy Policies. ACM. https://dl.acm.org/doi/pdf/10.1145/3178876.3186087

[39] Schlessinger, J and Day, D (2019, February 7). Most people just click and accept privacy policies without reading them — you might be surprised at what they allow companies to do. CNBC. https://www.cnbc.com/2019/02/07/privacy-policies-give-companies-lots-of-room-to-collect-share-data.html The comment in the article was made by Michael Kasdan, a partner at Wiggin and Dana, who specializes in privacy and intellectual property law.

[40] Ibid.

[41] Libert, T., page 207.

[42] Habib, page 9.

hard or impossible deletion processes".[43] Moreover, account deletion does not necessarily trigger deletion of all personally identifying information held by a company, which may not in fact occur or be very difficult for a consumer to accomplish.[44]

3. A large part of the consumer data ecosystem is invisible to Maryland consumers and trades in their personal information without anything they would recognize as consent. Most Maryland residents have little or no knowledge of the data broker companies compiling and holding detailed personally identifiable information about them and how their data flows among these companies and from them to ad firms and retailers. Consequently, consumers are not positioned to know their privacy policies and to exercise whatever options these companies may offer with respect to their data.

The data broker industry is vast and largely unregulated. Using state registries, Privacy Rights.org has identified 540 unique data brokers in the US.[45] For the most part, data brokers are not consumer facing and have unfamiliar names like Acxiom, AnalyticsIQ, Corelogic, and Experian Datacorp. Instead, as noted above, data brokers sell their detailed consumer profiles to retail firms and advertising platforms and may offer a variety of services to businesses, such as fraud detection and other risk mitigation services.

4. Marylander's personal information is at risk. The diffusion of sensitive Maryland consumer data across the commercial landscape creates certain risk exposures for them. These exposures include but are not exhausted by the following*:*

Data breaches. The most publicized exposure is to breaches and the harms that result from them. The list of companies that have had consumer personal information hacked is a long one, and the number of US consumers impacted is in the many hundreds of millions.[46] The PrivacyRights.org data breach database[47], which is sourced from notifications to states attorney generals, includes more than 9,000 breaches that affected more than 10 billion US consumer records over 14-year period (2005 – 2019). Closer to home, in 2021, the Maryland Attorney General's Office was notified of more than 1,400 breaches cumulatively affecting more than 600,000 reported State residents, with similar or larger numbers of residents affected in other years.[48] Certainly, many

[43] Habib, H., Pearman, S, et al (2020, April). "It's a scavenger hunt": Usability of websites' opt-out and data deletion choices. Page 3. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3313831.3376511

[44] Matsakis, L (2019, February 12). The WIRED guide to your personal data (and who Is using it). Wired. https://www.wired.com/story/wired-guide-personal-data-collection/ and Neilo, D (2019, November 7). How to opt out of the sites that sell your personal data. https://www.wired.com/story/opt-out-data-broker-sites-privacy/

[45] PrivacyRights.org (2022, February 22). Registered data brokers in the United States. https://privacyrights.org/resources/registered-data-brokers-united-states-2021. For its list of data brokers, see https://privacyrights.org/data-brokers?terms=&page=4

[46] The most recent reported data breach of this writing is of Transunion, a credit reporting agency. It is believed that the breach affected the names, addresses, full Social Security numbers, financial account numbers and driver's license information of more than 200 million customers. See the class action complaint against the company at https://www.classaction.org/media/bryant-v-trans-union-llc.pdf.

[47] The breach data is sourced from state Attorneys General and the U.S. Department of Health and Human Services. https://privacyrights.org/data-breaches

[48] See Office of the Maryland Attorney General, data breach snap shots for 2020, 2018, and 2016, respectively, at https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2020-snapshot-pdf.pdf, https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2018-snapshot.pdf, and

consumers have experienced multiple breaches of their personal identifying information, whether financial, medical, and/or other.

The harms to individuals from data breaches are many, including identify theft, consumer phishing and smishing scams[49], and sextortion.[50] The US Department of Justice estimated that for one year alone—2018—23 million US residents 16 years or older experienced identify theft. The large majority of these cases involved fraudulent use of credit cards that consumers were able to quickly resolve. However, 15% of the identity theft cases involved "account misuse" including attempted or completed misuse of savings or checking accounts and 17% concerned "misuse of personal information", including attempted or completed misuse to access medical care, purchase a home, or to accomplish other fraudulent purposes. For the 2018 year, the Department estimated losses exceeding $17 billion.

The new frontier in data breaches will involve biometric data as companies increasingly move to biometric modes of authentication and for commercial purposes, such as identifying VIP shoppers or patients, and biometrics begin to diffuse through the data ecosystem.[51] When breaches involve biometric data, they present a range of greater harms to consumers since unlike logins and passwords, biometric data cannot be reset. A recent report—*Leaked Today, Exploited for Life* —details a number of ways in which facial, voice, and fingerprint data can be used with other techniques to spoof authentication required to access bank accounts or devices, to identify, surveil and track individuals, to damage reputations by creating false contexts, and to engage in extortion, among many other harms.

Even companies that implement cybersecurity best practices can experience breaches. But certainly, many compromises are the result of deficient cybersecurity practices. Two well-known examples are the company, ID.me, which had contracts with the IRS, the Social Security Administration, and many state unemployment agencies to reduce fraud, and Equifax, the credit reporting agency.[52]

A more recent example is Suprema, a company which offers a web-based platform for using biometric data for facility access control, time and attendance management, facial recognition, and cybersecurity. Discovered by white hat hackers, a company server holding 23 gigabytes of biometric data was exposed for easy exploitation for an unknown period of time. The database "included pictures of end users attached to their facial recognition data, over a million records of

---

https://www.umgc.edu/content/dam/umgc/documents/upload/data-breaches-fy-2016-snapshot.pdf Note that "reported State residents" is not simply equivalent to unique individuals since breaches are reported independently. A given resident may have been affected by more than one breach.

[49] Leonhardt, M (2021, March 23). Consumers lost $56 billion to identity fraud last year—here's what to look out for. CNBC. https://www.cnbc.com/2021/03/23/consumers-lost-56-billion-dollars-to-identity-fraud-last-year.html. The article reports that most of the losses due to consumer fraud in 2020, $43 billion, stemmed in part from consumer scams using phishing attacks.

[50] Doffman, Z (2020, February 1). Ashley Madison hack returns to 'haunt' its victims: 32 million users now watch and wait. https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait/?sh=7bb95b9a5677

[51] See the collection if white papers at Biometric Update.com, https://www.biometricupdate.com/white-papers

[52] See the FTC submission by the Center for Democracy and Technology (2022, November 21). In the matter of Trade Regulation Rule on Commercial Surveillance and Data Security. Page 66. https://cdt.org/insights/cdt-comments-to-ftc-regarding-prevalent-commercial-surveillance-practices-that-harm-consumers/

fingerprint data, username and password combinations in plain text including some for administrative accounts, client employee records including personal identifiable information, and records of entry and exit at client facilities"[53] The researchers noted that user names and passwords were unencrypted, that fingerprints were not hashed and could be copied, and that the data could be edited and new users added.[54]

5. Consumers are exposed to the risk that their personal information will be used in ways that are inconsistent with privacy policies or legal requirements. Actions by the Federal Trade Commission and a number of states provide examples in this connection. In the matter of Flo Health, Inc, the FTC alleged that despite promising to keep this sensitive health data private, the company shared the data from millions of users of its Flo Period & Ovulation Tracker app with marketing and analytics firms, including Facebook and Google."[55] The settlement required the company to notify users about the disclosure of their health information and to instruct the third parties involved to destroy the data and prohibited the company from engaging in various forms of misrepresentation, including the purposes of its data collection and the control that consumers have over the data.

The development of facial recognition algorithms involves mapping and storing meta data on faces in a manner that makes them identifiable. In an action involving Everalbum, Inc, the Commission alleged that the company "deceived consumers about its use of facial recognition technology [on user photos uploaded to the app] and its retention of the photos and videos of users who deactivated their accounts".[56] Among the terms of the settlement, the company was required "to clearly and conspicuously disclose, and obtain consumers' affirmative express consent for all purposes for which it will use or share User's Biometric Information before using the information to create data needed for face recognition analysis or to develop face recognition models or algorithms" and "to delete (A) photos and videos of Ever app Users who requested deactivation of their accounts, (B) face recognition data that it created without obtaining Users' affirmative express consent, and (C) models and algorithms it developed in whole or in part using images from Users' photos."[57]

[53]Doffman, Z (2019, August 21). New data breach has exposed millions of fingerprint and facial recognition records. Forbes. https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=5de3e6f246c6

[54] Ibid.

[55] Federal Trade Commission Press Release (2021, June 22). FTC finalizes order with Flo Health, a fertility-tracking app that shared sensitive health data with Facebook, Google, and Others. https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

[56] Federal Trade Commission Press Release (2021, January 11). California company settles FTC allegations It deceived consumers about use of facial recognition in photo storage app. https://www.ftc.gov/news-events/news/press-releases/2021/01/california-company-settles-ftc-allegations-it-deceived-consumers-about-use-facial-recognition-photo

[57] The Federal Register (2021, January 1). Everalbum, Inc.; Analysis of proposed consent Order to aid public comment. https://www.federalregister.gov/documents/2021/01/25/2021-01430/everalbum-inc-analysis-of-proposed-consent-order-to-aid-public-comment

States such as Illinois, Louisiana, and Texas have also pursued cases alleging that the use of is without consumer consent and violates their biometric privacy statutes.[58]

6. There are impacts on consumers of incorrect personal information. Consumer exposure also exists where large consumer profiles include incorrect information. This is true of the three principal credit bureaus[59], although in this case consumers may be more aware of how to monitor and correct their profile and have rights under statute to challenge negative credit decisions based on erroneous information. In other cases, consumers may be less aware that incorrect data about them exists until they suffer negative consequences requiring time and effort to address. An example is the negative impact of incorrect information surfacing in a background check for employment.[60] More recently, much has been written about the problems with facial recognition technology and concerns about their deployment for a broad range of commercial purposes, including identification of shoppers, fraud detection and loss prevention, among others.[61]

Recommendations to Support Consumer Trust in Maryland

Recommended are certain foundational principles for affording greater protection of consumer privacy in a digital world and contributing to a relationship of trust between consumers and companies that collect and use their data.[62] At the front end, these principles provide for:

[58] See Nash, J. (2022, December 1). Consumers in three recent biometric data privacy cases seek class action. Biometric Update.com. status; Roth, E. (2022, June 6). Google to pay $100 million to Illinois residents for Photos' face grouping feature. https://www.theverge.com/2022/6/6/23156198/google-class-action-face-grouping-biometric-information-illinois-privacy-act; National Law Review (2022, October 20). First Jury Verdict Issued in Illinois Biometric Privacy Act Class Action. https://www.natlawreview.com/article/first-jury-verdict-issued-illinois-biometric-privacy-act-class-action, and Reuters (2022, October 20). Texas sues Google for allegedly capturing biometric data of millions without consent. https://www.reuters.com/legal/texas-sues-google-allegedly-capturing-biometric-data-millions-without-consent-2022-10-20/

[59] US Consumer Finance Protection Bureau (2021, September 1). What are common credit report errors that I should look for on my credit report? https://www.consumerfinance.gov/ask-cfpb/what-are-common-credit-report-errors-that-i-should-look-for-on-my-credit-report-en-313/

[60] Steiner, Erin. (2013, January 7). 5 Stories of background checks gone awry. https://www.huffpost.com/entry/5-stories-of-background-c_b_2427586

[61] Government Accounting Office. Facial Recognition Technology (2020, July). https://www.gao.gov/assets/gao-20-522.pdf

[62] For the diffusion of these principles among discussions of consumer rights, see White House (2021), idem, especially Appendix A.; Consumer Reports and epic.org (2022, January 26). How the FTC can mandate data minimization through a Section 5 Rulemaking. https://advocacy.consumerreports.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; Center for Democracy and Technology (2022, November 21). Submission to the Federal Trade Commission in the matter of Trade Regulation Rule on Commercial Surveillance and Data Security. Section II. https://cdt.org/wp-content/uploads/2022/11/CDT-Comments-to-FTC-on-ANPR-R111004.pdf; The Electronic Frontier Foundation, et al (2022, August 23). Comments to the California Privacy Protection Agency on Proposed Rulemaking Under the California Privacy Rights Act of 2020. https://privacyrights.org/sites/default/files/2022-09/California%20Privacy%20Rights%20Act%20Proposed%20Rulemaking%20-%20Comments%20to%20the%20California%20Privacy%20Protection%20Agency%20-%208-23-22.pdf; as well submissions to the Ad Hoc Subcommittee on Consumer Privacy by Commonsense.org.

- Greater consumer awareness of who holds their data, including not only companies with which they have a consensual relationship but also data brokers. Recommended in this connection is a State registration requirement for data brokers as implemented in Vermont and other states.
- Greater consumer control over what data is collected by companies with which they interact and how it is used, including the option to opt-out of data sharing or selling to third parties
- Transparent and understandable privacy policies to enable consumers to easily exercise these choices
- Data collection, use, and retention that is consistent with the consumer's relationship with the company and what is needed to provide services to the consumer

With respect to data held by companies:

- Consumers should have access to the data companies hold on them in a format that the consumer can understand (data portability)
- Consumers should have the right of rectification or the right to correct information that is in error
- Subject to certain legal restrictions, consumers should be able to delete all of their data held by a company, including all data compiled by the company regardless of source, and that the deletion should extend to third-party recipients of the consumer's data
- Companies should be required to have data security practices reasonably commensurate with the sensitivity of the data held

With respect to enforcement:

- Accountability through appropriate mechanisms and penalties to ensure that the principles are observed

These principles do not relieve all challenges confronting the consumer, such as the multiplicity of privacy policies and the lack of a true global data deletion option that would remove sensitive consumer data throughout the ecosystem. But recognizing these limitations, the principles can improve the consumer's position vis-à-vis the collection and use of their data. Furthermore, the implementation of these principles in some form is not impractical. Public concern is driving momentum among governing bodies to legally codify these principles in some measure. This is true not only for EU citizens under the General Data Protection Regulation (GDPR) but also now for consumers in five states, including California, Colorado, Utah, Virginia, and most recently, Connecticut.[63]

Finally, this means that many companies, certainly the largest ones, and the one collecting and using the most data, already are implementing them for specific populations. Codifying these principles would extend them to Maryland residents.

[63] See Appendix A for an analysis of the state laws referenced and a discussion of federal privacy legislation.

Section II: Digital Child Privacy as a Special Case

While the consumer privacy principles discussed above are applicable to data collected on children, there are issues specific to children that this section discusses. The governing federal statute pertaining to the activity of children online and the related responsibilities of companies is the Children Online Privacy Protection Act (COPPA). While a crucial step forward in in protecting children online, there have been calls to strengthen the regulatory framework in the light of issues that experience with the framework have revealed. As is the case with general consumer protection, the likelihood that these issues will be addressed at the federal level are difficult to assess but can and are being addressed at the state level. This section provides an overview of COPPA and related issues and recommendations.

COPPA Overview

COPPA was passed in 1998 and is the principal federal legislation protecting children. The Federal Trade Commission (FTC) is the implementing agency. It published its first rule in 2000 and updated it in 2013.

The COPPA protections extend to the online collection of "personal information" of children under the age of 13.[64] It is an important distinction that COPPA does not regulate the content of the site that may be considered inappropriate for a child to access.[65] The rule applies to three categories of "operators":[66]

- "Commercial websites and online services (including mobile apps and IoT devices) directed to children under 13 that collect, use, or disclose personal information from children."
- "General audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information of children under 13."
- "Websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children."

These definitions are intended to be broad, pacing with the changing nature of the online space. Included are "services that allow users to play network-connected games, engage in social networking activities, purchase goods. or services online, receive online advertisements, or interact with other online content or services. Mobile applications that connect to the Internet, Internet-enabled gaming platforms, connected toys, smart speakers, voice assistants, voice-over-Internet protocol services, and Internet-enabled location-based services also are online services covered by COPPA."[67]

[64] Federal Trade Commission (July 2020). Complying with COPPA: Frequently Asked Questions. https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions. Subsequent references to FAQs are to this source.
[65] FAQ A11
[66] FAQ A1, A2.
[67] FAQ A5

The cornerstone of COPPA's strategy for protecting the privacy of children's personal information is the requirement of verifiable parental consent to the information policies of covered sites and services.[68] So that parents can exercise this control, operators must post a "clear and comprehensive" online privacy statement that must address elements stipulated by the FTC.[69] These include identifying what data will be collected, how it will be used, permit verifiable parental consent, and allow parents to withdraw that consent at a later time.

Under COPPA, "personal information" includes the following:[70]

- First and last name
- A home or other physical address including street name and name of a city or town
- Online contact information
- A screen or user name that functions as online contact information;
- A telephone number
- A Social Security number
- A persistent identifier that can be used to recognize a user over time and across
- different websites or online services
- A photograph, video, or audio file, where such file contains a child's image or voice
- Geolocation information sufficient to identify street name and name of a city or
- town; or
- Information concerning the child or the parents of that child that the operator
- collects online from the child and combines with an identifier described above

The COPPA rule provides for a safe harbor program for self-regulating industry groups that create their own guidelines approved by the FTC through its notice and comment process as meeting or exceeding COPPA requirements.[71] To date, the FTC has approved eight of these groups including Children's Advertising Review Unit (CARU), Entertainment Software Rating Board (ESRB), iKeepSafe, kidSAFE, Privacy Vaults Online, Inc. (d/b/a PRIVO), and TRUSTe.

COPPA-related Issues

There are two significant issues that are explored here with respect to COPPA.

One concerns the collection of the personal information of children under 13 where, for very different reasons, verifiable parental consent does not occur prior to collection and use. One of these cases involves general audience sites—e.g., social media sites, dating apps—whose terms of service prohibit the participation of these children. Personal information collection happens because a) children misrepresent their age during the site registration process, and b) COPPA law does not impute "knowledge" to operators that would require them to obtain parental consent under the law when data they already have demonstrates they should know children are

[68] FAQ I. Note that COPPA permits schools to consent in loco parentis for online services in the "educational context". Apart from schools, there are other carefully circumscribed exceptions to parental consent. See FAQ N and J.
[69] FAQ A1, A2, and FAQ C.
[70] FAQ A7.
[71] FAQ O.

on the platform. Consequently, the collection of personal information of children without prior verifiable parental consent happens as it would for any other users without triggering COPPA requirements. The question is whether these platforms should be required where possible to obtain parental consent prior to the collection of personal information of children on their platforms. To do this would involve a change in the knowledge standard applicable to them. The other case in this category involves child-directed sites which fail to adhere to COPPA requirements, including the posting of privacy policies and enforcing verifiable parental consent prior to the collection of personal information.

Apart from these cases, the other major COPPA-related issue discussed below concerns children and targeted advertising.

1. Issues Around the Collection of Children's Personal Information

General audience sites and the actual knowledge standard. Apart from websites or services that are child-directed and that collect, use, or disclose personal information, other websites that have "actual knowledge" that they are collecting personal information of children under 13 are subject to COPPA. What constitutes actual knowledge? The FTC has offered a number of indicators.

- A site or service is deemed to have actual knowledge if a child under 13 discloses her age and the site or service is aware of it.[72]
- Apart from age disclosure, the FTC assumes actual knowledge in other cases. Several examples suffice. Notification from a concerned parent that makes clear the age or grade of the child using a site constitutes actual knowledge.[73] The actual knowledge standard is likely met when an ad network has been notified or receives a signal that the personal information it is collecting via cookies or other means is from child-directed sites. Likewise, the standard applies if a representative of the ad network recognizes the child-directed content of sites where ads are placed.[74] The same can be true for platforms that host third-party content and collect personal information from users of those channels. Actual knowledge is assumed if they are notified by the third-party that the content is child-directed or if the platforms themselves rank or characterize content as directed to children under 13.[75]

The FTC states that general audience sites can "block" children under 13 from participating if they so choose. Major general audience platforms such as Facebook, Twitter, TikTok, Instagram have taken this approach. They have terms of service that prohibit children under 13 from participating and require that age be provided in the site registration process. The FTC has

[72] FAQ H6.
[73] Ibid.
[74] FAQ E1
[75] FTC Business Blog (September 4, 2019). $170 million FTC-NY YouTube settlement offers COPPA compliance tips for platforms and providers. https://www.ftc.gov/business-guidance/blog/2019/09/170-million-ftc-ny-youtube-settlement-offers-coppa-compliance-tips-platforms-and-providers. See also *FTC et al vs Google LLC* (2019) and the FTC's complaint and the federal district court's permanent injunction and civil penalty order at https://www.ftc.gov/legal-library/browse/cases-proceedings/172-3083-google-llc-youtube-llc

provided guidelines to online sites and services to help minimize falsification of age.[76] Further, it has stated that "an operator of a general audience site or service that chooses to screen its users for age in a neutral fashion may rely on the age information its users enter, even if that age information is not accurate."[77]

COPPA was passed when parental supervision was comparatively easy to exercise. The home computer was the way in which families accessed the internet, and parents could look over the shoulders of their children to see what they were doing online. With the evolution of the internet, the appearance of mobile devices and the apps, children are able to access online content wherever they are and whenever they want making it more difficult for parents to know what their children are doing online.

Consequently, it is not surprising that children under 13 are to be found on sites whose terms of service bar them. This is true of social media platforms which have an attraction for children.[78] A methodologically careful survey of American children found that a significant percentage of them participate on these platforms.[79]

Age-Gated Platform (Terms of Service Require Users to be At Least 13 Years Old)	Percent Use at Least Once Per Day (Children Aged 9 – 12)
Facebook	45%
Instagram	40%
Snapchat	40%
TikTok	41%
Twitter	30%
WhatsApp	39%

The research noted that what is true of social media sites is also true of dating apps.[80] Specifically, while these apps require users to be 18 or older, the study reported that 14% of girls and 27% of boys aged 9 – 12 in its sample used these apps.

All these apps collect data that is defined as personal information by COPPA. This includes not only inputs of the child, such as an email address, or information that they may share about themselves or their families, or photos and videos that they may post, but other information of which they are likely not aware: persistent identifiers, granular GPS location, and residential IP address. This information is combined with other data, like browsing history, that persistent

[76] FAQ H3
[77] FAQ A12
[78] Rogers, K (October, 2021). Children under 10 are using social media. Parents can help them stay safe online. CNN at https://www.cnn.com/2021/10/18/health/children-social-media-apps-use-poll-wellness/index.html and Thorn (2020). Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking at https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf
[79] Thorn, idem, Figure 4. Note that the table above is a subset of social media apps that the research considers. The study distinguishes Facebook from Facebook Messenger for Kids. See also the Mott Poll Report. Sharing Too Soon: Children and Social Media Apps. (October, 2021) at https://mottpoll.org/sites/default/files/documents/101821_SocialMedia.pdf
[80] Thorn, idem, p. 17. The dating apps in the survey included Bumble, Grindr, and Tinder, with "other" as an option.

identifiers enable these platforms and their networks to track. But again, this data collection on children under 13 happens without triggering COPPA requirements and without liability. This is because these sites are age gated and post terms of service that require the user to be 13 years old or older. They are within the law to accept the users' self-reported age.

Child-directed sites and COPPA compliance. It has been reported that by age 13 the ad tech industry holds about 72 million data points on the average child.[81] This data collection starts well in advance of their participation on social media platforms.

Pixalate is "fraud protection, privacy, and compliance analytics platform for Connected TV (CTV), Mobile Apps, and Websites".[82] As part of its practice, Pixalate periodically evaluates what it assesses to be child-directed apps in the Google Play Store and Apple App Store for COPPA compliance risk.[83] The key risk factors for child-directed apps comprise what "personal information" is collected (e.g., granular GPS coordinates, IP address), whether the apps have privacy policies, and whether the apps request permission to collect other sensitive information (e.g., voice, photographs, videos).

Given the number of apps, Pixalate analysis of them is mostly automated. A small subset of the most popular apps is manually inspected for compliance risk by its Trust and Safety Advisory Board[84]. The risk continuum consists of low, medium, high, and critical.[85] Pixalate is careful to say that its findings represent its "opinions" and are "not guarantees or facts".[86] Its analysis is intended as a flag for compliance review. Nonetheless, it is worth noting that academic research discussed below has resulted in findings that raise similar COPPA compliance questions about child-directed apps.[87]

The Q2 2022 analysis by Pixalate found that there are more than 422,000 likely child-directed apps in Google and Apple stores.[88] A subset of the Q2 findings are below.

	Google	Apple
Total Likely Child-directed Apps	270, 818	152,107
Likely Child-directed apps with….		
*Undetected Privacy Policy	27,427	24,209

[81] Cross, Tim (December, 2017). Ad Tech Collects 72 million data points on the average American child by age 13. VideoWeek. https://videoweek.com/2017/12/14/ad-tech-collects-72-million-data-points-on-the-average-american-child-by-age-13/

[82] From Pixalate's website at https://www.pixalate.com/

[83] For Pixalate's methodology, see https://www.pixalate.com/coppa-compliance-tools-methodology and https://www.pixalate.com/knowledgebase/coppa-data-dictionary

[84] See https://www.pixalate.com/trust-and-safety-advisory-board

[85] See " PIXALATE'S OVERALL COPPA RISK ASSESSMENT METHODOLOGY" on its methodology page cited above.

[86] Idem., see "Disclaimer".

[87] See Ryes, I., et al (2018). Won't someone think of the children? Examining COPPA compliance at scale. Proceedings on Privacy Enhancing Technologies:18 (3):63–83. https://www.researchgate.net/publication/324864696_Won't_Somebody_Think_of_the_Children_Examining_COPPA_Compliance_at_Scale

[88] Pixalate's Q2 2022 COPPA Risk Scorecard Report: Google vs. Apple can be downloaded at https://www.pixalate.com/blog/q2-2022-coppa-risk-scorecard-report

*Requests Permission to Access Personal *Info in Order for App to Operate	119,376	58,160
*GPS Transmitted to the Ad Industry	23,774	11,809
Residential IP Address Transmitted to The Ad Industry	14,900	8,420

As Pixalate categorizes risk, an undetected privacy policy is per se categorized as "critical". Without a privacy policy, there is no information about what data is collected and how it is used or shared, all clearly required by COPPA. Pixalate categorizes as high risk an app that requests sensitive permissions to operate (like access to camera or microphone) and transmits either residential IP address and/or geolocation, even if a privacy policy is detected. Similarly, it categorizes as high risk an app that does not request sensitive permissions to operate and transmits such information, again, even where a privacy policy is detected.[89]

These high-risk categorizations reflect a limitation of Pixalate's tool. The tool cannot detect whether apps require verifiable parental consent prior to app use. Given the sensitivity of personal information, Pixalate elects for an evaluation that would more likely trigger a compliance review.

However, other research supports the assumption that many child-directed apps in fact do not require verifiable parental consent. In 2018, researchers reviewed 5,855 child-directed apps in the Google Play Store using a tool that they devised. They found that that 73% transmitted sensitive data over the internet, and that "none of these apps attained to the level of verifiable parental consent". [90] The researchers reached this conclusion because their tool demonstrated that those apps could be opened and used through simple taps and swipes. Dr. Serge Egelman, one of the researchers, summed up their most concerning findings in Senate testimony in 2021:

> In terms of the most serious privacy violations, we observed that roughly 300 of the apps that we tested (4.8%) were collecting children's contact information (e.g., names, email addresses, and phone numbers) and/or precise location data, which included apps specifically targeted at children under 5. In most cases, this data was transmitted to third-party advertising companies, or third parties that otherwise support the advertising industry. I believe that this is a serious finding that should be put in perspective: roughly 1 in 20 of the apps that we examined were collecting information without the requisite verifiable parental consent, and for which the FTC has previously brought cases.[91]

With respect to the transmission of child data without verifiable parental consent, Dr. Egelman noted that this could be due to a combination of factors. It could be error (app developers using

[89] See "Risk Scores" at https://www.pixalate.com/coppa-compliance-tools-methodology
[90] Reyes, I, Wijesekera, P, et al (2018) "Won't somebody think of the children?" Examining COPPA compliance at scale. Proceedings on Privacy Enhancing Technologies. See page 69. https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf
[91] Egelman, S. (May 18, 2021). Testimony before the United States Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, and Data Security, p. 4. https://www.commerce.senate.gov/services/files/0DC78E9D-88B2-4D54-8F4A-AE7B4C7D0EF6

portions of their code (SDKs) from libraries and not correctly setting the permissions so that they neither collect nor transmit information). It could also be due to developers' ignoring terms of service attached to SDKs and using software components that are not intended for use in child-directed apps.

Among other shortcomings, Dr. Egelman and his researchers underscored the lack of security in many child-directed apps in the data transmission itself.

> The most common issue that we observed was the transmission of personal data using insecure means. Under COPPA, covered services are required to "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children." While neither the statute nor regulations define what are considered "reasonable procedures," Transport Layer Security (TLS) and its predecessor have been industry standards more than three decades now; its use is required on U.S. government websites.
>
> Simply put, it is not considered "reasonable" to transmit personal information without the use of TLS to secure it. Nonetheless, we observed that 40% of the children's apps (2,344 apps) we tested failed to take this reasonable procedure.
>
> What this means is that for users of these apps, their personal information is accessible to any eavesdroppers.[92]

It must be noted that the Apple Store and the Google Play Store do require developers to adhere to COPPA-informed design guidelines for inclusion in smaller, branded subcategories of child-directed apps within their stores to assist parents.[93] While an important initiative, findings such as the foregoing raise questions about the scale of these initiatives and whether more can be done to enforce COPPA requirements in the design and functioning of child-directed apps across these stores.[94]

Use Case: Child-directed Site and Lack of Verifiable Parental Consent

Within Google Play Store is a family of more than 180 mostly panda-themed apps by BabyBus, a Chinese company. App titles include "Baby Panda Care, "Little Panda Toy Repair Master",

---

[92] Egelman, idem, page 7.

[93] Perez, S (2020, April 15). Google Play adds a 'Teacher Approved' section to its app store. Tech Crunch. https://techcrunch.com/2020/04/15/google-play-adds-a-teacher-approved-section-to-its-app-store/?guccounter=1&guce_referrer=aHR0cHM6Ly9kdWNrZHVja2dvLmNvbS8&guce_referrer_sig=AQAAAEgd-kQ4VkUTTgO9iZ8Oth7em4bZhYWXS_aBzvFG-1DnA9fDsRMbaJ-FYwCGBf-eXiWHZ5_szXmTBug21RA-HeazySsqjjYp0rtZtpIh9p-PXl4vo48bdD3G7K7l3tPSLvYYHRvibyRxQNtHB-J31rTFZ88iMAJvNWUr8zm2XSbZ and Perez, S (2013, September 22). Introducing Apple's New "Kids" App Store https://techcrunch.com/2013/09/22/introducing-apples-new-kids-app-store/

[94] See Pixalate (2022, March 2). 80% of American Parents Worry About Children's Online Privacy, but Only 48% Monitor Activity Regularly". Pixalale's CEO stated the two app stores "only provide a target age range for 200 apps at a time" and noted that "Pixalate's research shows there are nearly 400,00 child-directed apps in the Google and Apple app stores, about 40% of which collect sensitive data like geolocation." He went on to state that the "poll results beg the question of whether the app operators [the children] are doing this with parental consent as required by COPPA."

"Little Panda Sweet Bakery", "Little Panda's Puppy Pet Care", "Baby Panda Jewel Adventure", among many others. The company's privacy policy (data safety/details/developer privacy policy) recognizes that a child may be the first one to see the app and improbably directs the child to seek parental consent.[95] The policy states (emphasis in the original):

> **If you are a minor child or under the legal age to consent, please read the following privacy policy with your parent. Also, you must obtain parental consent before playing our Apps**.
>
> BabyBus is committed to protecting the privacy of children who use our Apps. This privacy policy explains our information collection, disclosure, and parental consent practices concerning the information provided by children. Accordingly, this Privacy Policy aims to comply with the requirement of the U.S. Children's Online Privacy Protection Act ("COPPA"), the General Data Information Protection Regulation and("GDPR") and any other applicable laws. We reserve the right to amend this Privacy Policy.

The policy states in Section 1 that the apps collect certain personal information passively—IP address and device identifiers. In addition to the data collected by BabyBus, the policy also references "information collected by third parties".

In this connection, Section 2 observes that ad tech technologies are built into the apps to enable the apps to be offered free of charge. But as the default, the policy states that BabyBus has tried to disable the collection function while cautioning that BabyBus does not "fully guarantee" that these data collection technologies are disabled. As an additional precaution, the reader is directed to disable the collection of device identifier "when prompted by an authorization notice" or by taking additional steps on the device's settings. As for the personal information that it collects, BabyBus states in Section 3 that it does not sell the data to any third parties but that it may disclose or allow the data to be used by its affiliated companies with consent as "applicable under law".

Parental rights are described in section 5 of the policy:

> • At any time, parents can refuse to permit us to collect further personal information from their children and can request that we delete the personal information we have collected in connection with that account. Please keep in mind that a request to delete personal information may lead to the deletion of an account.
> • Parents can request access to and delete their children's personal information by logging into the children's account.
> • Parents can also contact us to request access to, change, or delete their child's personal information by sending an email to us at privacy@babybus.com.

Despite the provision of a way for parents to contact BabyBus, its apps have no mechanism to enforce verifiable parental consent prior to the use of the app. Meanwhile, BabyBus apps collect

[95] The policy is shared here.

information that COPPA defines as "personal information" and without intervention, the apps allow sharing of this information with third-party advertisers.

In a test for this report using "Bay Panda Jewel Adventure", it was found that the ad feature is the *default* and that the parent or child must solve a multiplication problem to disable this permission. When the ad disabling feature was accessed, Google Play indicates that it will cost $1.99 to use the app without ads. In using the app without changing the default, ads for shoes, a K8 academy, and other products and services quickly began to appear.

2. Targeted advertising. The use of apps by children exposes them to a variety of harms. Targeted advertising has been linked to some of them. Targeted advertising is driven by algorithms that process data harvested from users, profile them, and provide users content which take a variety of forms meant to influence. These can be ads, videos, memes, or, on social media platforms, feeds from accounts that are suggested to the user to follow.

The harm to children comes from the fact that the younger they are, they are not aware of the data collected about them, they do not understand that ads are customized to them, and they are not able to critically evaluate advertising, whether the ads are about products (e.g., snacks) or body image, or that groom them in subtle ways for other behaviors, such as gambling. "Children's readiness to learn from the social world renders them vulnerable."[96] This is especially true if the ads are presented by cartoon characters, other children, celebrities, or other influencers. Effects can include including negative eating habits, poor self-image, depression, unhealthy behaviors, and suicidal thoughts.[97]

These findings have been well documented with respect to the promotion of eating disorders by Instagram. In research published in 2022[98], Fairplay found that there are over 90,000 unique pro-eating disorder accounts on Instagram reaching 20 million unique followers. A third of the users were underage and some as young as nine or ten. As the research notes, in a widely covered experiment, Senator Blumenthal's office created a fake Instagram account for a 13-year-old girl following a few dieting and eating disorder accounts. The Senator stated that "[w]ithin a day its recommendations were exclusively filled with accounts that promote self-injury and eating disorders. That is the perfect storm that Instagram has fostered and created."[99]

---

[96] Lapierre, Mathew A et al (2017). The effect of advertising on children and adolescents. Pediatrics. Vol 140, p. 153. https://publications.aap.org/pediatrics/article/140/Supplement_2/S152/34178/The-Effect-of-Advertising-on-Children-and?autologincheck=redirected?nfToken=00000000-0000-0000-0000-000000000000

[97] See for example, American Psychological Association (2004). Report of the APA Task Force on Advertising and Children. https://www.apa.org/pi/families/resources/advertising-children.pdf; The American Psychological Association (2010). The impact of food advertising on childhood obesity. https://www.apa.org/topics/obesity/food-advertising-children; and the American Academy of Pediatrics (2020). Digital advertising to children. https://publications.aap.org/pediatrics/article/146/1/e20201681/37013/Digital-Advertising-to-Children, and Fairplay (2021). Designing for Disorder: Instagram's Pro-eating Disorder Bubble. https://fairplayforkids.org/pf/designing-disorder/

[98] Fairplay, idem.

[99] Parsley, A. (2021, October). People. https://people.com/politics/senator-poses-teen-girl-instagram-finsta/. See also Grabe S, et al (2008). The role of the media in body image concerns among women: a meta-analysis of experimental and correlational studies. Psychological Bulletin. Vol 134(3), p. 460. https://www.researchgate.net/publication/5259131_The_Role_of_the_Media_in_Body_Image_Concerns_Among_Women_A_Meta-Analysis_of_Experimental_and_Correlational_Studies

As Frances Haugen's Senate testimony and background documents indicated, Meta (Instagram's owner) had allowed this advertising to occur even while being aware of its harm.[100] Fairplay estimates that Meta made more than $227 million from all those who follow pro-eating disorder accounts on Instagram, $.5 million directly from underage accounts, and $62 million from those who follow the underage pro-eating disorder accounts.[101]

This practice is not limited to Meta. Google and its YouTube are another example. YouTube channels have been established by popular toy makers like Hasbro and Barbie and by numerous other content creators with a child-directed focus. The FTC showed in federal court that Google and YouTube were aware that these channels were child-directed, that they nonetheless collected COPPA-defined personal information of the users, and that they sold targeted advertising on these sites. From the small number of child-directed channels that the FTC reviewed, it estimated that Google and YouTube earned close to $50 million in advertising revenue. The total advertising revenue from the universe of those channels was certainly far more. The $170 million judgement against Google and YouTube was the largest that the FTC had won in an enforcement action.[102]

Recommendations to Enhance the Digital Privacy and Protection of Children in Maryland

The body of research by academics and public interest advocacy organizations validates the concerns of parents. Echoing earlier polls, a 2022 Pixalate-Harris poll found that 80% of parents are concerned about their children's privacy when using apps with 73% concerned about their children's location being tracked.[103] The result has been a number of policy recommendations to strengthen child privacy online which have been incorporated into legislation at the state level and in proposed bills at the federal level. At a minimum, this report recommends the following for Maryland:

- **Require constructive knowledge in lieu of actual knowledge as the standard against which general audience apps and other platforms are held to determine whether they must comply with children's online protections**. As a general matter, constructive knowledge would mean that given the data practices of an "operator" as defined by COPPA, it would be reasonable to assume that the operator knew or should have known children are using their platform

[100] Frances Haugen (2021, October 4). Testimony before United States Senate Committee on Commerce, Science and Transportation, Sub-Committee on Consumer Protection, Product Safety, and Data Security. https://www.commerce.senate.gov/index.php/services/files/FC8A558E-824E-4914-BEDB-3A7B1190BD49 and Wells, G, Horwitz, J, and Seetharaman, D (2021). Wall Street Journal. Facebook knows Instagram is toxic for teen girls, company documents show. https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

[101] Fairplay, idem, Executive Summary and p. 13.

[102] See Note 76 above.

[103] Pixalate (2022, March 2). 80% of American parents worry about children's' online privacy, but only 48% monitor activity regularly. https://www.prnewswire.com/news-releases/80-of-american-parents-worry-about-childrens-online-privacy-but-only-48-monitor-activity-regularly-301494258.html. Parental concerns have been captured in polls going back 10 or more years.

- **Engage Apple and Google representatives about expanding the scope of efforts to minimize child-directed apps in their stores that are not COPPA compliant.**
- **Ban targeted advertising on child-directed apps.** This recommendation aims to address the harms to children from targeted advertising that have been identified in subcommittee testimony.[104]
- **Require data minimization with respect to data collected on children**. Data minimization is a general privacy recommendation of the Federal Trade Commission[105] and is advocated as a practice with respect to children's data.[106] It would require operators to limit data collection to what is reasonably necessary to provide a product or service, to be transparent about the specific purpose of the data collection no later than the time of collection, and to retain data only for the period of time necessary to process a transaction or to provide a service.
- **Rectification and deletion rights.** Already a right for consumers in general in five states, this recommendation would specifically extend these rights to children's data in Maryland.
- **Security**. Similarly, consistent with consumer privacy principles and legislation in other states, mandate security standards for data collected and transmitted on children that are reasonably commensurate with the sensitivity of the data.

At the state level, California's Consumer Privacy Rights Act[107] and its new Age-Appropriate Design Code Act[108] implement the foregoing recommendations.

In the current Congress, a number of bills have been to strengthen COPPA or otherwise provide additional protection of children's privacy.[109] These bills reflect a bipartisan concern that current law provides insufficient safeguards. These bills include Protect Kids Act (HR 1781, Representative Tim Walberg [R]), Protecting the Information of our Vulnerable Children and Youth Act (HR 5703, Rep Kathy Castor [D]), Children and Teens Online Privacy Act (S 1628. Sen Edward Markey [D] and Sen Bill Cassidy [R]), and the Kids Online Safety Act (S 3663, Senator Sidney Blumenthal [D]). It is unlikely that these bills will pass, leaving it to the states to provide additional protections to children.

[104] Ibid, pp. 7-8. See also Haley, H (2022, August 23). Testimony before the Ad Hoc Subcommittee on Consumer Privacy, Maryland Cybersecurity Council, p.5. https://1drv.ms/b/s!AjqEqIxJkAfagdd7GY7Tt37azAatJQ?e=BO3kbv and

[105] Federal Trade Commission (2015, January). Internet of things: privacy in a connected world. https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

[106] See for example, Ly, I (2022, August 23). Testimony before the Ad Hoc Committee on Consumer Privacy, Maryland Cybersecurity Council. https://1drv.ms/b/s!AjqEqIxJkAfagddBIdWyGonkdklDEQ?e=IwZdOc

[107] See https://www.caprivacy.org/cpra-text/

[108] AB 2273. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

[109] See https://cdp.cooley.com/us-legislative-developments-in-childrens-privacy/

Section III. Convenings of the Subcommittee Contributing to the Record

The Ad Hoc Subcommittee on Consumer Privacy received outside presentations and comments from the following through its summer and fall meetings. These were provided by the following:[110]

August 23, 2022
Irene Ly, Policy Counsel, Common Sense Media
Haley Hinkle, Policy Counsel, Fairplay
Phyllis Marcus, Partner, Hunton Andrews Kurth LLP

September 22, 2022
The Honorable Rob Bonta, Attorney General of California
Amy Gajda, The Class of 1937 Professor of Law, Tulane University Law School
Bethany Corbin, Senior Counsel, Nixon Gwilt Law

October 20, 2022
Maureen Mahoney, Deputy Director of Policy and Legislation, California Privacy Protection Agency.

November 18, 2022
Andrew Kingman, Mariner Strategies LLC, representing the State Privacy and Security Coalition
Quinn Laking, Third-year Law Student, University of Maryland School of Law, and Legal Intern at the Center for Health and Homeland
Security, University of Maryland
Nikita Vozenilek, Third-year Law Student, University of Maryland School of Law, and Legal Intern at the Center for Health and Homeland Security, University of Maryland

Section IV: Questions and Comments about the Report

Questions and comments may be address to:
University of Maryland Global Campus
ATTN Maryland Cybersecurity Council Staff
3501 University Boulevard East
Adelphi, Maryland 20783
Marylandcybersecuritycouncil@umgc.edu

[110] See Note 2 for links for recordings of each of the meetings.

APPENDIX A

OVERVIEW OF CONSUMER PRIVACY RIGHTS LEGISLATION AT THE STATE AND FEDERAL LEVELS

Overview of State Consumer Privacy Rights Legislation

Quinn Laking
Third-year Law Student, University of Maryland School of Law
Legal Intern, Center for Health and Homeland Security
University of Maryland

I. Introduction

With an absence of federal legislation regulating consumer privacy, states have introduced and passed laws to protect their citizens' data privacy in the marketplace. Since 2018, five states (California, Colorado, Connecticut, Virginia, and Utah) have passed comprehensive consumer privacy laws.[111] As of August 11th, 2022, four additional states (Michigan, New Jersey, Ohio, and Pennsylvania) have active bills in committee which follow the example of the five states with statutory consumer privacy laws. A further twenty-five states, including Maryland, have introduced data privacy bills that are no longer active for various reasons. These introduced and passed State Privacy Acts confer both consumer rights and business obligations, utilizing a two-prong approach to protect consumers' data privacy.

II. Consumer Rights

Consumer rights, the first prong in State Data Privacy Acts, explicitly grant consumers data rights to access, rectification, deletion, restriction, portability, opt out of sales and/or automated decision making, and, sometimes, a private right of action. This bundle of rights empowers the consumer to be informed about their data's collection and, in many cases, control business's use of that data to some extent.

A. Right to Access, Portability, Rectification, and Deletion of Personal Information

Ubiquitous across all states with active or inactive privacy bills and laws, was a consumer's right to access. This right empowers a consumer to access the information or categories of information collected about a consumer from a business or data controller. This includes access to information or categories of information the business or data controller shares with third parties. This right ensures the consumer is knowledgeable about the data collected and who it is shared with. This knowledge also ensures transparency between the business or data controller and the consumer.

Almost ubiquitous across all states with active or inactive privacy bills was the consumer's right of portability, which works hand and hand with the consumer's right to access. The right of portability is the consumer's right to have their collected personal information provided to them by the collecting business or data controller in an easy to read and easily accessible format. Once again, this is to ensure transparency between the consumer and the business. The consumer can then provide that information to another business or data collector if they so choose.

The right to rectification is the consumer's right to request personal information collected by a business or data collector be corrected if the information collected is incorrect. This is not the

[111] The majority of the data used in this Comprehensive Consumer Privacy Law summary is provided by the International Association of Privacy Professionals (IAPP). This data can be found on their webpage "US State Privacy Legislation Tracker". US State Privacy Legislation Tracker 2022, IAPP, Last Updated: October 7, 2022.

same as the right to deletion, which is detailed below. Of the nine states with active privacy bills or laws, only Utah did not include the right to rectification. Of the states with inactive privacy bills, only four out of twenty-three states did not include a right to rectification in the proposed bill.

Finally, all nine states with active data privacy bills or laws, and almost all states with inactive privacy bills included the right to deletion. This right is the final logical step in empowering the consumer to control their personal information collected by businesses. The right of deletion guarantees a consumer the right to request deletion of their collected data under certain circumstances. The bills and laws vary on the scope of this right and include some exceptions.[112] For example, the California privacy law defines the deletion right as the right to request deletion for any data collected from the consumer. By contrast, the Virginia law gives the consumer the right to request deletion of any data collected from or *obtained about* the consumer. The Virginia law gives the consumer the ability to request deletion of information they did not provide to the business or data collector, but that the business obtained from another source. The exceptions to the deletion request vary but generally include complying with law, performing security or investigative functions, identifying, or repairing bugs in the functionality of the business's electronic systems, and solely for internal uses that are reasonable given the context under which the consumer provided the information.

B. Right to Opt-Out of Sales and Automated Decision Making

Almost ubiquitous across all states with active or inactive privacy bills and laws was the right to opt-out of sales. The right to opt-out of sales, also known as the Right to No Sale, is the consumer's right to restrict or prohibit the business or data collector's sale of their collected personal information to third parties for value or profit.

Seven of the nine states with active privacy bills and laws included the right to opt-out of at least some automated decision making. Automated decision making is when a business uses an automated process, without human input, to make decisions about a consumer based on their collected information. The goal of this right is to protect the consumer from the sometimes-discriminatory effects of artificial intelligence or machine learning when there is no human guidance or oversight of the decision-making process.[113]

C. Private Right of Action

Only four of the nine states with active privacy bills or laws included provisions for a private right of action against businesses or data collectors who do not comply with the state's data privacy law. This provision allows individual consumers to bring civil suits against businesses for violations of the data privacy statute. Of those four states, three of them only created a private right of action under limited circumstances. Around half of the states with inactive data privacy bills included some private right of action in its proposed law. Generally, the creation of a private right of action is not typically included in a state's data privacy laws, with only California including it under limited circumstances. It remains to be seen if New Jersey and Pennsylvania's bills pass with this provision included.

---

[112] "Consumers' "Right to Delete" under US State Privacy Laws" by Glenn A. Brown. March 3, 2021. https://www.consumerprivacyworld.com/2021/03/consumers-right-to-delete-under-us-state-privacy-laws/

[113] "Biden must act to get racism out of automated decision-making" by ReNika Moore. August 9, 2021. https://www.washingtonpost.com/opinions/2021/08/09/biden-must-act-get-racism-out-automated-decision-making/

III. Business Obligations

Business obligations, the second prong in State Data Privacy Acts, creates affirmative responsibilities for any business collecting consumers' personal data. These obligations create an environment friendly towards consumer data privacy and operates as a set of standards that businesses must comply with without the need for an invocation of consumer rights.

A. Opt-In Default Age Requirement

All states with active or inactive privacy bills and laws, except for Arizona, incorporated an opt-in by default age requirement. Generally, this provision of the bill or law requires a business to make data collection sales an "opt-in" feature, rather than an "opt-out" feature. Consequently, by default, when a consumer interacts with a business the collected information will not be sold until the consumer has given permission for the business to use their data for profit. Each state's provision varied in its specific requirements, limiting the requirement by age or by information type.

Over two-thirds of states with active or inactive data privacy bills limited the opt-in default requirement by age. This requires businesses to protect young consumers' data from sale, but older consumers would not need to be provided with an opt-in feature by default. The age threshold ranges from 13 to 18, depending on the state. A handful of states with inactive bills had no age requirement, instead the opt-in by default feature was required for everyone of all ages. It is notable, however, that of the five states with active data privacy laws, only opt-in default provisions that were limited by age passed into law. All five states set the age requirement at either 13 or 16, where consumers over this age did not need to be given the opt-in default.

Some states limited the opt-in default by sensitivity of information sold, instead of or in conjunction with an age requirement. Sensitive data is defined differently by each state in their local laws but typically involves all personal information of children and sensitive information of adults. Of the five states with active data privacy laws, three of them only require an opt-in by default for the sale of sensitive information. In those three states, the sale of a consumer's non-sensitive personal information is presumptively allowed, but the consumer must opt-in to the sale of their sensitive information. Around half of the states with inactive privacy bills proposed an opt-in by default requirement for sensitive information, usually in conjunction with an age requirement. From all of the above data it can be seen that states are prioritizing preventing the sale of children's sensitive data by requiring businesses to provide an opt-in option by default for data sales.

B. Notice Requirement, Prohibition on Discrimination, and Purpose Limitation

Ubiquitous in all states with active or inactive privacy bills or laws is a notice requirement for businesses. This requirement obliges a business to provide notice to consumers about certain data privacy practices of the business. This provision codifies an already common practice for most businesses and ensures consumers are aware of each business's data collection policies.

Ubiquitous in all states with active data privacy bills or laws and extremely common in states with inactive data privacy bills is the prohibition against discrimination for consumers asserting their data privacy rights. This provision ensures consumers can assert their data privacy rights without being treated differently by the business from consumers who choose not to assert those rights. Consequently, data privacy rights are strengthened and more likely to be used by consumers when no retaliatory action can be taken by the business.

All nine states with active data privacy bills or laws, except Utah, include a purpose limitation provision. The purpose limitation borrows from the EU's General Data Protection Regulation and prohibits the collection of personal information except for a specific purpose. The states with inactive data privacy bills also very frequently contained a purpose limitation requirement. This provision generally holds businesses accountable for informing the consumer of the purpose behind collecting the consumer's data, and then following through on that communication by using the collected data as they stated it would be used and not for another purpose. This provision is grounded in fair information practices and aligns with the FTC's efforts to hold businesses accountable when they misuse consumer's information.[114]

C. Risk Assessment

Finally, seven of the nine states with active data privacy bills or laws required businesses to conduct formal risk assessments on their data privacy practices. This provision was less common in the states with inactive data privacy bills with only half of the states writing this requirement into the bill. This imposed duty requires businesses to prioritize their data privacy practices and should ensure better adherence to the statute because the business is periodically reviewing their own practices.

IV. Conclusion

California, Colorado, Connecticut, Virginia, and Utah are leading the nation in protecting their citizen's data privacy, with a further thirty states entertaining data privacy laws of their own. In general, these data privacy laws establish formal consumer data privacy rights and place positive obligations on businesses to proactively process and protect consumers' data.

Within active state laws, consumer rights of access, deletion, portability, and the right to opt-out of sales are ubiquitous in all five states, with the right of rectification and the right against automated decision making not present in the Utah statute alone. A private right of action is featured only in California's law, and only under limited circumstances. All five states require businesses to provide a sales opt-in feature by default for children under a certain age, as well as a notice to consumers of all ages about the business's data practices. All five states also prohibit businesses from discriminating against consumers for asserting their data privacy rights. Finally, all five states, except Utah, require formal risk assessments of data privacy practices and limit the business's collection of data to their stated purpose for collection.

In states with either active bills or inactive bills for data privacy, some combination of consumer rights and business obligations has been proposed. In general, rights of access, portability, and opt-out of sales is the most common. Business obligations for an opt-in feature by default for the sale of children's data and notice requirements is the most common.

[114] *Statement of Commissioner Rohit Chopra: Regarding the Report to Congress on the FTC's Use of Its Authorities to Protect Consumer Privacy and Security*. Commission File No. P065404. June 17, 2020. https://www.ftc.gov/system/files/documents/public_statements/1577067/p065404dpipchoprastatement.pdf

Overview of Privacy-related Bills Proposed in 117th Congress

Nikita Vozenilek
Third-year Law Student, University of Maryland School of Law
Legal Intern, Center for Health and Homeland Security
University of Maryland

Children and Teens' Online Privacy Protection Act, S 1628 / American Data Privacy and Protection Act (ADPPA), H.R. 8152 / Consumer Online Privacy Rights Act (COPRA), S. 3195 / Data Care Act of 2021, S. 919 /Online Privacy Act of 2021 (OPA), H.R. 6027 /Control Our Data Act (CODA)

Table I. Comparison of Individual Rights[115]

	CTOPPA 1628	**ADPPA**	**COPRA**	**Data Care Act**	**OPA**	**CODA**
Access	§4(a)(5)	§203(a)(1)	§102(a)	Silent	§101	§102(c)(1)(B)
Correction	§4(a)(6)(B)(iv)	§203(a)(2)	§104	Silent	§102	§102(c)(1)(C)
Deletion	§4(a)(5)	§203(a)(13)	§103	Silent	§103	§102(c)(1)(D)
Opt Out	silent	§204	§105(b)	Silent	§28(b)	§102(c)(1)(E)
Portability	silent	§203(a)(4)	§105(a)	Silent	§104	Silent

Table II. Comparison of Obligations[116]

	CTOPPA	**ADPPA**	**COPRA**	**Data Care Act**	**OPA**	**CODA**
Notice	§3(a)(9)	§202(e)	§102(b)	Silent	§210	§102(b)
Affirmative Consent for Sensitive Info	§3(a)(9)(A)	§103(a)(3)(A)	§105(c)	Silent	§210	§103
Privacy Policy	§8(b)(4)	§202(a)	§102(b)	Silent	§211	§102(a)
Minimization	§9(b)(2)(C)(ii)	§101	§106	Silent	§§201-202	§§104-105
Data Security	§8(b)(1)-§9(b)(2)(C)	§208	§107	§3(b)(1)(A)	§212	§109
Breach Notices	Silent	Silent	Silent	§3(b)(1)(B)	§213	Silent

[115] CTOPPA; and CRS, based on information in the ADDPA, COPRA, Data Care Act, OPA, and CODA (https://crsreports.congress.gov/product/pdf/LSB/LSB10776)
[116] CTOPPA; and CRS, based on information in the ADDPA, COPRA, Data Care Act, OPA, and CODA (https://crsreports.congress.gov/product/pdf/LSB/LSB10776)

Children and Teens' Online Privacy Protection Act, S 1628: Introduced by Sen. Ed Markey (D-MA) and Sen. Bill Cassidy (R-LA). Introduced in Senate committee on Commerce, Science and Transportation.[117] This proposal amends the Children Online Privacy Protection Act (COPPA) of 1998 to "strengthen protections relating to the online collection, use and disclosure of personal information of children and minors, and for other purposes" this update would extend the laws rule to children through the age of 17. The bill prohibits an operator of a website, online service or application, or mobile application directed to a minor with constructive knowledge that the user is a minor from collecting personal data without: (1) providing notice and obtaining consent; (2) providing a parent or minor with specific information upon request; (3) conditioning participation by a user on the provision of personal information and; (4) establishing and maintaining reasonable procedures to protect the personal information collected from users.

The bill further outlines principles governing how operators should collect and use personal information, along with providing information to a parent or minor, who must be able to challenge the accuracy of personal information that must be ultimately corrected by the operator. Mechanisms for the erasure of elimination of personal information must be available and made privy to users. In addition, to prohibiting targeted marketing directed to minors without their consent, the bill further prohibits the sale of internet-connected devices targeted to minors unless they meet certain cybersecurity and data security standards. Manufactures of such devices must display a privacy dashboard detailing how personal info is collected and used. This bill would establish a Youth Marketing and Privacy Division at the Federal Trade Commission (FTC).

The Statute on which CTOPPA expands, COPPA, was originally intended to govern how websites and online services protect the privacy of children under 13 years of age and is enforced by the Federal Trade Commission. Chairwomen of the Senate Committee on Commerce, Science and Transportation Sen. Maria Cantwell (D-WA) noted that this "bill would close a loophole that had been allowing companies to abuse the data of children with little accountability and make it harder for the FTC to prove violations." Though the proposed legislation seems to guarder much support from Senate Democrats, Senate Republicans are also concerned about privacy protections. At start of the CTOPPA hearing in the Senate, Ranking member Sen Wicker said he would not support CTOPPA because "the need for a national law that provides data protections for everyone must be this committee's priority…while no legislation is perfect, the ADPPA represents a bipartisan, bicameral compromise that I believe has the best chance of reaching the president's desk by the end of the year."[118]

The **American Data Privacy and Protection Act** (ADPPA) was introduced by Rep. Frank Pallone (D-NJ) into the House Committee on Energy and Commerce.[119] This bill is intended to establish requirements for how companies handle personal data, including information that identifies or is "reasonably linkable" to an individual. The bill requires companies to limit the collection, processing and transfer of personal data which is reasonably necessary to provide a requested service or product. The bill establishes consumer data protections, including the right to access, correct, and delete personal data. Prior to engaging in targeted advertising, the bill requires companies to provide individuals with a means to opt out of such advertising. The bill

[117] https://www.congress.gov/bill/117th-congress/senate-bill/1628/text
[118] https://iapp.org/news/a/us-senate-committee-advances-two-childrens-privacy-bills/
[119] https://www.congress.gov/bill/117th-congress/house-bill/8152/text

also provides additional protections with respect to personal data of individuals under the age of 17. It further prohibits companies from using personal data to discriminate based on specified protected characteristics.

Additionally, companies must implement security practices to protect and secure personal data against unauthorized access, and the Federal Trade Commission (FTC) may issue regulations for complying with this requirement. The bill provides for enforcement of these requirements by the FTC and state attorneys general. Beginning four years after the bill's enactment, individuals may, subject to certain notification requirements, bring civil actions for violations of the bill. The bill preempts state laws that are covered by the provisions of the bill except for certain categories of state laws and specified laws in Illinois and California.

The Consumer Online Privacy Rights Act (COPRA): Introduced by Sen. Maria Cantwell (D-WA) in the Senate Committee of Commerce, Science and Transportation.[120] This bill applies to entities that process or transfer consumer data and requires that the Federal Trade Commission establish a new bureau to assist in the enforcement of its provisions. The bill requires entities to: (1) make their privacy policy publicly available and provide an individual with access to their personal data; (2) delete or correct, upon request, information in an individual's data; (4) export, upon request, an individual's data in a human-readable and machine-readable format; (5) establish data security practices to protect the confidentiality and accessibility of consumer data; and (6) designate a privacy officer and a data security officer to implement and conduct privacy and data security programs and risk assessments. In addition, the bill prohibits such entities from: (1) engaging in deceptive or harmful data practices; (2) transferring an individual's data to a third party if the individual objects; (3) processing or transferring an individual's sensitive data without affirmative express consent; (4) processing or transferring data beyond what is reasonably necessary or for which they have obtained affirmative express consent; (5) processing or transferring data on the basis of specified protected characteristics (such as race, religion, or gender); (6) conditioning the provision of a service or product on an individual's agreement to waive their privacy rights; and (7) retaliating against an employee who provides information about a potential violation of the bill's provisions, or who testifies or assists in an investigation or judicial proceeding concerning such a violation. The bill was introduced in the Senate Committee of Commerce, Science and Transportation by Sen. Maria Cantwell (D-WA)

The Data Care Act of 2021 was sponsored by Sen. Brian Schatz (D-HI) and introduced into the Senate Committee on Commerce, Science and Transportation.[121] This bill would impose "various duties" This bill imposes various duties on online service providers with respect to their handling of individual-identifying data that can be reasonably linked to a specific user. The bill notes that online service providers have a duty to: (1) reasonably secure such data from unauthorized access; (2) refrain from using such data in a way that will result in reasonably foreseeable harm to the end user, and (3) not disclose such data to another party unless that party is also bound by the duties established in this bill. Further, the bill authorizes the Federal Trade

[120] https://www.congress.gov/bill/117th-congress/senate-bill/3195/text
[121] https://www.congress.gov/bill/117th-congress/senate-bill/919/text

Commission and specified state officials to take enforcement actions regarding breaches of these duties.

Online Privacy Act of 2021 (OPA) H.R. 6027: Introduced by Rep Anna G. Eshoo (D-CA) into the House - Energy and Commerce and the Committees on the Judiciary and House Administration.[122] This bill establishes certain online privacy rights for personal information (including contents of communications) and certain requirements for covered entities, data processors, service providers, and third parties. Individual rights include rights regarding of access, correction, deletion, portability, human review of automated decisions, individual autonomy, to be informed, impermanence. The bill establishes noted exemptions and exceptions including for example, amongst others, such as protecting public safety, protecting a legally recognized privilege or right, precenting security incidents, threats and deceptive or fraudulent activity. The bill also establishes the Digital Privacy Agency, and independent agency in the executive branch, to enforce such rights and requirements.

Control Our Data Act (CODA)[123]: This bill would establish consumer privacy protections and data security for individuals whose personal information is collected, used, and shared by certain entities to require safeguards on the collection and use of such information and restrictions on the sharing of such information, to properly safeguard their data, and to amend the Federal Trade Commission Act to implement various reforms to the Commission's practices, and for other purposes.

[122] https://www.congress.gov/bill/117th-congress/house-bill/6027/text

[123] https://republicans-energycommerce.house.gov/wp-content/uploads/2021/11/2021.11.02-Republican-CODA-Draft-.pdf