

THE COMMONWEALTH OF MASSACHUSETTS OFFICE OF THE ATTORNEY GENERAL

ONE ASHBURTON PLACE
BOSTON, MASSACHUSETTS 02108

MAURA HEALEY
ATTORNEY GENERAL

(617) 727-2200
www.mass.gov/ago

November 17, 2022

Via Online Submission

Federal Trade Commission, Office of the Secretary
600 Pennsylvania NW, Suite CC-5610 (Annex B)
Washington, DC 20580

RE: Commercial Surveillance ANPR, R111004

We, the Attorneys General of Massachusetts, Connecticut, Illinois, New Jersey, North Carolina, and Oregon, joined by the respective Attorneys General of the undersigned states, write to the Federal Trade Commission (“FTC” or “Commission”) in response to the August 22, 2022 Advanced Notice of Proposed Rulemaking (“ANPR” or “Notice”) (FTC-2022-0053-0001) on Commercial Surveillance and Data Security. As the chief consumer protection officials in most of our respective states, we hope to inform the Commission as it contemplates new trade regulation rules governing commercial surveillance and data security.

The State Attorneys General commend the FTC for its comprehensive review of corporate surveillance and data security in preparing the Notice. We, too, are concerned about the alarming amount of sensitive consumer data that is amassed, manipulated, and monetized. Our offices frequently receive outreach from consumers concerned about the privacy and security of their information. Research supports that consumers are worried about commercial surveillance and feel powerless to address it.¹ Many consumers believe that tracking by companies is inevitable, yet often do not even know what is being recorded.² These fears intensify when they learn more about the commercial surveillance economy,³ and in particular consumers fear falling victim to identity theft and data misuse.⁴ A majority doubt that their data can be kept secure.⁵ Contributing to these concerns is the fact that companies are often collecting more data than they can effectively manage or need to perform their services.⁶

Our consumer privacy-related enforcement actions and investigations have resulted in settlements that have provided significant business practice changes to strengthen data security and privacy going forward—but there is still more work to be done. Our submission highlights the heightened sensitivity of certain categories of consumer information, the dilemma of data brokers and how they surveil consumers, and how data minimization can help mitigate concerns surrounding data aggregation.

The Commercial Surveillance Economy Trades on Consumers' Sensitive Medical Data, Biometric Data, and Location Dataⁱ

Location Data

Location data is a particularly valuable commodity in the digital economy. An individual's location history reveals intimate details of daily life—such as where they live and work, their shopping habits, their daily schedule, or whether they visited the doctor or pharmacy. Even when aggregated or anonymized, location data is used by marketers and advertisers to take advantage of consumer behavior, for example, by predicting who is likely to visit a nearby store if only nudged by an advertisement, or by identifying the most vulnerable consumers.⁷ It can also be a proxy for improper discrimination, such as with digital redlining.⁸

Many consumers are not even aware that their location information is being collected. For instance, “free” apps often come with an obfuscated or little-disclosed cost of the transfer of a consumer's data. Consumers do not always understand under what circumstances they are being tracked in part because privacy policies and other representations are vague, confusing, go unread,⁹ or are unhelpful.¹⁰ Even when the uses for consumers' data are adequately disclosed, those promises often are not kept by developers, because app developers do not understand their own boilerplate privacy policies¹¹ or how their third-party tools might use data.¹²

When a consumer does wish to disable location sharing, their options are quite limited: turning off GPS location on a phone often is not enough, as Bluetooth,¹³ nearby wi-fi networks, IP addresses, or other identifiers are still used to determine location. Moreover, consumers who try to control location tracking within an app's settings may be deceived with dark patterns.¹⁴

States are recognizing the sensitive nature of this information. California, Connecticut, and Virginia all have laws which protect or restrict the use and collection of location data in some ways.¹⁵ These provide a framework to inform the Commission as it proceeds through the rulemaking process.

Biometric Data

The Commission should consider the risks of commercial surveillance practices that use or facilitate the use of facial recognition, fingerprinting, or other biometric technologies. At the most basic level, biometric data is biological data or characteristics about the unique behavioral and physical characteristics of individual persons.¹⁶ Companies collect various types of biometric data—including retina, face, and fingerprint scans—to authenticate and identify individuals. Companies collect employee biometric data for security purposes of entry, clocking in or out, and verification of identity.¹⁷ Many consumers provide this information to companies for security purposes or personal pursuits, such as to learn about their ancestry. But consumers are not always aware of when their data is collected, how it is used, or if it is resold for purposes to which they never meaningfully consented.^{18, 19}

ⁱ Addressing concerns generally raised in questions 10, 37, and 38 of the ANPR.

States are also recognizing the sensitive nature of this data, as evidenced by the Illinois Biometric Information Privacy Act (“BIPA”) and the Texas Capture and Use of Biometric Identifier Act (“CUBI”).^{20,21} Neither CUBI nor BIPA ban the capture of biometric data, but both provide safeguards and regulate the capture and use of this data in various ways.²² Similarly, the Colorado Privacy Act and Connecticut Data Privacy Act, both of which take effect in 2023, will require consent before the collection and use of personally identifying pieces of biometric data.²³

Medical Data

The Commission should consider the risks of commercial surveillance practices that use or facilitate the use of medical data, regardless of whether the data is subject to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). In our experience, HIPAA is deeply misunderstood by the general public.²⁴ Consumers do not understand what information HIPAA protects, or who must comply with HIPAA.²⁵ While the implementation of HIPAA resulted in the creation of the Privacy Rule to cover the use and disclosure of protected health information (“PHI”), the Privacy Rule only applies to PHI held by “covered entities,” a defined set of entities connected with the provision of health care.²⁶ Medical data not necessarily covered by HIPAA is often referred to as health adjacent data.²⁷ Examples of health adjacent data include data collected by wearables (such as smartwatches or heart monitors), health “Internet of Things” (“IoT”) devices (like smart scales, thermometers, pill dispensers, or sleep monitors), and health or wellness mobile applications.²⁸

Healthcare adjacent data is particularly sensitive, as it can be combined with other information to reveal intensely personal information. For instance, Google and other search engines store consumer internet queries, including health-related internet searches.²⁹ A unique personal identifier could be linked with a website search for key medical terms, such as HIV status, and then transmitted to 3rd party advertisers.³⁰

A recent article also revealed that Facebook was receiving appointment scheduling information from hospital websites through its tracker tool.³¹ Another report discovered that mental health applications could connect with several other companies, including Facebook.³² Small pieces of information transmitted in these ways can be aggregated into proxy data that allows companies to make assumptions and predictions about consumers. An example of the use of this proxy data occurred when Target could predict which of its customers were pregnant based upon who purchased unscented lotion.³³

Existing state privacy laws provide greater protection for healthcare adjacent data as they govern a broader swath of entities and information than HIPAA.³⁴ For example, the California Confidentiality of Medical Information Act’s (“CMIA”) definition of “provider of healthcare” extends to any business that offers hardware or software, “including a mobile application or related device”, that is designed to maintain medical information—covering certain health care applications and wearables that are not subject to HIPAA.³⁵ The law helps protect privacy by prohibiting publicly available information from being combined with individually identifiable information to create consumer profiles that would otherwise be treated as healthcare adjacent data. In 2020, for example, the California Attorney General enforced the CMIA against Glow, Inc.

for data security and consumer consent deficiencies involving Glow’s health-tracking application.³⁶

Data Brokers, and the Larger Surveillance Economy, Threaten Consumers’ Privacy, Security, and Liberty Interestsⁱⁱ

We echo the Commission’s observation in its ANPR that data brokers are a prominent part of the surveillance economy but remain largely invisible to consumers. Data brokers profile consumers by scouring social media profiles, internet browsing history, online and offline purchase history, credit card information, and government records, including driver’s license/motor vehicle records, census data, birth certificates, marriage licenses, and voter registration information. Data brokers also use this information to categorize consumers into audiences based on susceptibility to certain advertising or likelihood to buy certain products, such as “Thrifty Elders,” “Truckin’ & Stylin’,” or “Underbanked.”³⁷ These profiles—which can be purchased by almost anyone—can be used to dox,³⁸ swat,³⁹ stalk, and physically harm consumers.⁴⁰ Despite these severe harms, the data broker economy has ballooned in size and reach since the Commission last surveyed the industry in 2014.⁴¹

The unfairness endemic to the surveillance economy is perhaps best illustrated by how data brokers treat data collection versus data deletion. Data brokers do not need to obtain knowing and meaningful consent from consumers before tracking them and selling access to their profiles. Meanwhile, consumers who wish to opt out of data collection, processing, and monetization by data brokers must contact each of the relevant brokers separately, and, presuming the broker allows for and honors opt-out requests, provide them with the necessary information (often a government ID) to execute an opt-out. If the data broker does not permanently opt-out the consumer, the consumer will have to repeat this process every few months to ensure that data brokers do not simply recreate their consumer profile. The burden this presents to consumers demonstrates the asymmetric power wielded by data brokers and the overall exploitative nature of the industry.

Data brokers, technology companies, and other businesses also use surveillance technologies, including tracker software development kits (“SDKs”), advertising IDs, and tracking cookies to monitor consumers across time, space, and platforms.^{42,43,44,45,46} Consumers are rarely aware that these technologies exist or the breadth of data they can collect and transmit.⁴⁷ Once a company collects data using these technologies, it may then aggregate that information under an Advertising ID—a unique identifier that can track a consumer across the web.⁴⁸ Data brokers use these IDs to create consumer profiles built from information provided piecemeal to different websites or unknowingly collected from the consumer’s web browser. The danger of this scale of aggregation is its potential to deanonymize a consumer’s web activity. When multiple sets of data intersect, previously ‘anonymized’ but sensitive activity can easily be tied to individuals,⁴⁹ increasing the risk of targeted scams, unwanted and persistent advertising, identity theft, and lack of consumer trust in the websites they visit.

While advertisers may be starting to move away from third party cookies and tracking SDKs, the technology that replaces them should be met with some caution.⁵⁰ Advertising IDs and other new technology will likely continue to be used to collect information on individuals and

ⁱⁱ Addressing concerns raised in questions 41 through 50 of the ANPR.

serve targeted advertisements. For example, Google has developed the Privacy Sandbox, a tool which places consumers into advertising “cohorts” of similar search histories.⁵¹ Similarly, Apple has also introduced targeted advertising, using data collected from services attached to an AppleID.⁵² With the development of these new technologies, which still allow the largest companies to aggregate data on both populations and individual users, consumers and their data remain at risk.

Data Minimization May Mitigate Some of the Harms of the Commercial Surveillance Economyⁱⁱⁱ

It is vital that the Commission consider data minimization requirements and limitations. The prevailing “notice-and-choice” structure is largely failing consumers. Few consumers read privacy policies,⁵³ and even if they did, most policies “are long, complex, and often incomplete or silent on” data collection and sharing practices.⁵⁴ This means that such practices are “hard or simply impossible to learn.”⁵⁵ Moreover, as discussed in the recently released FTC Staff Report, *Bringing Dark Patterns to Light*, businesses frequently use “design elements that obscure or subvert consumers’ privacy choices.”⁵⁶ The result is that consumers are often coerced into sharing more personal data than they otherwise intended to.

With respect to data collection and retention, the Attorneys General encourage the Commission to examine the approach taken in the California, Colorado, Connecticut, Utah and Virginia consumer privacy laws. While the language varies among the laws, each statute mandates that businesses tie and limit the collection of personal data to what is “reasonably necessary” in relation to specified purposes.⁵⁷ The provisions in Colorado, Connecticut, and Virginia are consistent with Europe’s General Data Protection Regulation, which states that “[p]ersonal data shall be . . . adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”⁵⁸ California’s law goes a step further and applies a “reasonably necessary and proportionate” standard not only to collection but also to the “use, restriction, and sharing of a consumer’s personal information.”⁵⁹ This framework serves as a useful tool that could extend the protections enjoyed by a few states’ citizens to all Americans, and also ensure that businesses will be operationalizing known concepts.

Determining whether the collection, use, sharing, or retention of particular data is “reasonably necessary” or “reasonably necessary and proportionate,” will require a fact-specific inquiry, but the Commission could offer guidance to businesses through its prior orders and in the rule itself. The draft regulations proposed by the California Privacy Protection Agency provide one reference point for this type of guidance.⁶⁰ Those regulations, as modified following the public comment period, set forth factors for determining what qualifies as “reasonably necessary and proportionate” and further provide examples of what constitutes a consumer’s “reasonable expectations” with respect to the processing of their personal information.⁶¹ Colorado’s draft regulations concerning the secondary use of personal information similarly set forth a list of factors to consider when determining whether processing is “reasonably necessary to or compatible with” a specified purpose.⁶² The Attorneys General urge the Commission to study and potentially include illustrative examples of compatible and incompatible data practices.

ⁱⁱⁱ Addressing concerns raised in questions 43 and 47 of the ANPR.

Limiting the collection and retention of data by businesses will also improve consumer data security because businesses will have less data to protect and less data potentially available to threat actors in the event of an incident. The Attorneys General frequently investigate reported data breaches and often find that the impacted business failed to reasonably safeguard consumer data. Many breaches involve significant quantities of old or unused information or affect consumers who do not have ongoing relationships with the impacted business.⁶³ In some instances, prior to the breach, the business did not even know that it was storing personally identifiable information in a particular location.

For example, in January of this year, the New York Attorney General executed an Assurance of Discontinuance with EyeMed Vision Care, LLC, regarding a 2020 email account intrusion impacting approximately 2.1 million individuals.⁶⁴ According to the state’s findings, the breached account contained emails with consumer’s personal information dating back more than six years.⁶⁵ Then in June, 46 state Attorneys General entered into a settlement with Carnival Cruise Line regarding a 2019 “unstructured” data breach; unstructured breaches “involve personal information stored via email and other disorganized platforms” into which businesses lack visibility—resulting in unnecessary data retention.⁶⁶ As the cost of managed storage increases, businesses are turning to more unstructured data solutions, leading to further risk of unnecessary data retention.⁶⁷ Finally, in 2020, several states entered into a settlement with CafePress regarding a 2019 data breach in which “approximately 22 million accounts were affected, *including inactive and closed accounts*.”⁶⁸ The Commission’s recent complaint and order with CafePress regarding the same incident alleged that the company “created unnecessary risks to Personal Information by storing it indefinitely on its network without a business need.”⁶⁹

Each of these settlements included data retention and/or deletion requirements designed to ensure that the company would not unnecessarily retain consumer data going forward, leaving it vulnerable to compromise. Data minimization requirements may help businesses to prospectively evaluate and modify their data retention policies and schedules, mitigating potential future harms to consumers.

Conclusion

We thank the Commission for the opportunity to provide comment on the Commercial Surveillance ANPR. As a part of the rulemaking process, we encourage the Commission to consider how it can promote fairness, transparency, and accountability to consumers—and we hope the Notice leads to a Rule that serves as a critical tool to address misconduct and prevent consumer harm.

Respectfully Submitted,



MAURA HEALEY
Attorney General of Massachusetts



MATTHEW J. PLATKIN
Attorney General of New Jersey



WILLIAM TONG
Attorney General of Connecticut



JOSH STEIN
Attorney General of North Carolina



KWAME RAOUL
Attorney General of Illinois



ELLEN ROSENBLUM
Attorney General of Oregon



MARK BRNOVICH
Attorney General of Arizona



TODD ROKITA
Attorney General of Indiana



PHILIP J. WEISER
Attorney General of Colorado



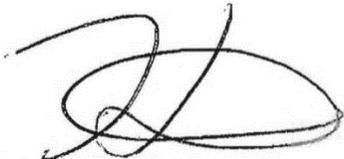
TOM MILLER
Attorney General of Iowa



KATHLEEN JENNINGS
Attorney General of Delaware



AARON M. FREY
Attorney General of Maine



KARL A. RACINE
District of Columbia Attorney General



BRIAN E. FROSH
Attorney General of Maryland



STEPHEN H. LEVINS
Executive Director
Hawaii Office of Consumer Protection



DANA NESSEL
Attorney General of Michigan



LAWRENCE G. WAsDEN
Attorney General of Idaho



KEITH ELLISON
Attorney General of Minnesota



AUSTIN KNUDSEN
Montana Attorney General of Montana



JOSH SHAPIRO
Attorney General of Pennsylvania



DOUG PETERSON
Attorney General of Nebraska



PETER NERONHA
Attorney General of Rhode Island



AARON D. FORD
Attorney General of Nevada



ALAN WILSON
Attorney General of South Carolina



JOHN M. FORMELLA
New Hampshire Attorney General



KEN PAXTON
Attorney General of Texas



HECTOR BALDERAS
Attorney General of New Mexico



SEAN REYES
Attorney General for Utah



LETITIA JAMES
Attorney General of New York



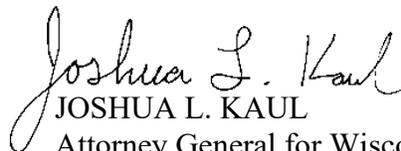
SUSANNE R. YOUNG
Attorney General for Vermont



JOHN O'CONNOR
Attorney General of Oklahoma



BOB FERGUSON
Washington State Attorney General



JOSHUA L. KAUL
Attorney General for Wisconsin

Citations

¹ “72% of Americans are reluctant to share information with businesses because they “just want to maintain [their] privacy.” Tim Morey et al., *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV. (May 2015), <https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust>.

² Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

³ “We find evidence of significant dispersion and heterogeneity in valuations before the information intervention, with women and Black and low-income individuals reporting systematically lower valuations than other groups. After an information intervention, we detect significant revisions in valuations, concentrated among individuals with low initial valuations.” Avinash Collis et al., *Information Frictions and Heterogeneity in Valuations of Personal Data* (Nov. 30, 2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974826.

⁴ 76% of respondents to one survey were “worried” about identity theft, and 34% were “very worried.” Generali Global Assistance, *Consumers Find ID Theft More Concerning than Serious Illness or Injury*, PR NEWSWIRE (May 18, 2021), <https://www.prnewswire.com/news-releases/consumers-find-id-theft-more-concerning-than-serious-illness-or-injury-301293401.html>.

⁵ Mary Madden & Lee Rainie, *Americans’ Attitudes About Privacy, Security and Surveillance*, PEW RSCH. CTR. (May 20, 2015), <https://www.pewresearch.org/internet/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

⁶ Jarret Jackson, *Businesses Have More Data Than Ever Before, But Do They Measure What They Manage?*, FORBES (July 15, 2020), <https://www.forbes.com/sites/jarretjackson/2020/07/15/businesses-have-more-data-than-ever-before-but-do-they-measure-what-they-manage/?sh=2e6c45ca693a>.

⁷ See e.g., STAFF OF S. COMM. ON COM., SCI., & TRANSP., 113TH CONG., A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES (Dec. 18, 2013), <https://www.commerce.senate.gov/services/files/bd5dad8b-a9e8-4fe9-a2a7-b17f4798ee5a> (identifying data brokers’ products that identify financially vulnerable consumers, some of which include: “Rural and Barely Making It,” “Ethnic Second-City Strugglers,” “Retiring on Empty: Singles,” “Tough Start: Young Single Parents,” and “Credit Crunched: City Families”).

⁸ CBS NEWS, *Justice Department to Investigate “Digital Redlining” in Lending*, (Oct. 22, 2021), <https://www.cbsnews.com/news/justice-department-redlining-investigation-digital-racist-practices/>.

⁹ Auxier et al., *supra* note 2.

¹⁰ Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were An Incomprehensible Disaster*, N.Y. TIMES: THE PRIVACY PROJECT (June 12, 2019), <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

¹¹ For example, developers can now “generate” privacy policies, further decreasing their need to engage with the policies’ terms and what they mean. See e.g., *Privacy Policy Generator*, TERMLY, <https://termly.io/products/privacy-policy-generator/> (last visited Sept. 29, 2022).

¹² See section below, *Data Brokers, and the Larger Surveillance Economy, Threaten Consumers’ Privacy, Security, and Liberty* Interests, for a general discussion on SDKs. See, e.g., Complaint, Flo Health, Inc., F.T.C. File No. 1923133 (June 17, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_complaint.pdf (noting that despite repeated representations that it would keep users’ health data secret, Flo Health shared health data to numerous third-party marketing and analytics firms through SDKs integrated into the Flo app); see also *Snyk Exposes Malicious iOS SDK That Breached User Privacy For Millions and Performed Ad Fraud in Thousands of Apps*, PR NEWSWIRE (Aug. 24, 2020), <https://www.prnewswire.com/news-releases/snyk-exposes-a-malicious-ios-sdk-that-breached-user-privacy-for-millions-and-performed-ad-fraud-in-thousands-of-apps-301116756.html>.

¹³ Michael Kwet, *In Stores, Secret Surveillance Tracks Your Every Move*, N.Y. TIMES: THE PRIVACY PROJECT (June 14, 2019), <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html>. As one example, Walmart’s privacy policy instructs visitors to “adjust your device’s Bluetooth settings to completely disable the collection of Bluetooth location-related data” if they desire privacy. See *Privacy Policy*, WALMART, <https://corporate.walmart.com/privacy-security/walmart-privacy-policy> (last updated July 11, 2022). Similarly, CVS’s privacy policy instructs consumers to completely “disable[e] Bluetooth on your mobile device.” See *Privacy Policy*, CVS, https://www.cvs.com/help/privacy_policy.jsp (last updated July 18, 2022).

-
- ¹⁴ See Att’y Gen. of Ill. et al., Comment Letter on F.T.C. Request for Information on Digital Advertising Business Guidance Publication (Aug. 2, 2022), <https://www.regulations.gov/comment/FTC-2022-0035-0024>.
- ¹⁵ California Privacy Rights Act (CPRA), CAL. CIV. CODE § 1798.100(c) (2020) (effective Jan. 1, 2023), <https://www.caprivacy.org/cpra-text/>; An Act Concerning Personal Data Privacy and Online Monitoring, S.B. 6, Gen. Assemb., Reg. Sess. (Conn. 2022) (effective July 1, 2023), <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF>; Virginia Consumer Data Protection Act, Va. Code Ann. §§ 59.1-575 to 59.1-585 (effective Jan. 1, 2023), <https://law.lis.virginia.gov/vacode/title59.1/chapter53/>.
- ¹⁶ Sterling Miller, *The Basics, Usage, and Privacy Concerns of Biometric Data*, THOMSON REUTERS (July 20, 2022), <https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data>.
- ¹⁷ Jake Holland, *As Biometric Lawsuits Pile Up, Companies Eye Adoption With Care*, BLOOMBERG L. (Feb. 9, 2022), <https://news.bloomberglaw.com/privacy-and-data-security/as-biometric-lawsuits-pile-up-companies-eye-adoption-with-care>.
- ¹⁸ Louise Matsakis, *The WIRED Guide To Your Personal Data (And Who Is Using It)*, WIRED (Feb. 15, 2019), <https://news.bloomberglaw.com/privacy-and-data-security/as-biometric-lawsuits-pile-up-companies-eye-adoption-with-care>.
- ¹⁹ *As part of the Settlement in ACLU v. Clearview AI, the Company is Now Permanently Banned, Nationwide, from Making Its Faceprint Database Available to Most Businesses and Other Private Actors*, ACLU (May 9, 2022), <https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois>.
- ²⁰ Biometric Information Privacy Act (BIPA), 740 ILCS 14/1 *et seq.* (2008), <https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>.
- ²¹ Capture and Use of Biometric Identifier (CUBI), TEX. BUS. & COM. CODE § 503.001 (2021), <https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm>.
- ²² Rachel Metz, *Here’s Why Tech Companies Keep Paying Millions to Settle Lawsuits in Illinois*, CNN BUSINESS (Sept. 20, 2022), <https://www.cnn.com/2022/09/20/tech/illinois-biometric-law-bipa-explainer/index.html>.
- ²³ Consumer Privacy Act, Col. Rev. Stat. § 6-1-1301, *et seq.* (effective July 1, 2023), https://coag.gov/app/uploads/2022/01/SB-21-190-CPA_Final.pdf, Connecticut Data Privacy Act, Pub. Act No. 22-15 (effective July 1, 2023), <https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF>.
- ²⁴ Health Insurance Policy and Accounting Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936, <https://www.congress.gov/bill/104th-congress/house-bill/3103>.
- ²⁵ Lydia Wheeler, *Confusion Over Health Privacy Law Seen Impeding Covid Battle*, Bloomberg L. (Aug. 17, 2021), <https://news.bloomberglaw.com/health-law-and-business/confusion-over-health-privacy-law-seen-impeding-covid-battle>.
- ²⁶ *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, C.D.C., <https://www.cdc.gov/php/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient%27s%20consent%20or%20knowledge> (last updated June 27, 2022).
- ²⁷ Tawanna Lee & Antonio Reynolds, *All Data Is Not HIPAA Data – Healthcare Covered Entities Should Pay Close Attention to State Privacy Laws Regulating the Health IoT Ecosystem*, JDSUPRA (July 13, 2021), <https://www.jdsupra.com/legalnews/all-data-is-not-hipaa-data-healthcare-3523068/#:~:text=Healthcare%20data%20that%20does%20not%20constitute%20PHI%20or,and%20healthcare%20applications%20often%20fall%20within%20this%20category>.
- ²⁸ *Id.*
- ²⁹ Geoffrey Fowler, *Okay, Google: To Protect Women, Collect Less Data About Everyone*, WASHINGTON POST (July 1, 2022), <https://www.washingtonpost.com/technology/2022/07/01/google-privacy-abortion/>.
- ³⁰ Tatum Hunter & Jeremy Merrill, *Health Apps Share Your Concerns with Advertisers. HIPAA Can’t Stop It.*, WASHINGTON POST (Sept. 22, 2022), <https://www.washingtonpost.com/technology/2022/09/22/health-apps-privacy/>.
- ³¹ Todd Feathers & Simon Fondrie-Teitler, *Meta Faces Mounting Questions from Congress on Health Data Privacy As Hospitals Remove Facebook Tracker*, THE MARKUP (Sept. 19, 2022), <https://themarkup.org/pixel-hunt/2022/09/19/meta-faces-mounting-questions-from-congress-on-health-data-privacy-as-hospitals-remove-facebook-tracker>.
- ³² Thomas Germain, *Mental Health Apps Aren’t All As Private As You May Think*, CONSUMER REPORTS (Mar. 2, 2021), <https://www.consumerreports.org/health-privacy/mental-health-apps-and-user-privacy-a7415198244/>.

-
- ³³ Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>.
- ³⁴ See e.g. Colorado Privacy Act, COL. REV. STAT. § 6-1-1303(24), which includes “Personal Data revealing... a mental or physical health condition or diagnosis...” as Sensitive Data.
- ³⁵ Confidentiality of Medical Information Act (CMIA), CAL. CIV. CODE §§ 56.10 – 56.16, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV.
- ³⁶ Press Release, California Office of the Attorney General, *Attorney General Becerra Announces Landmark Settlement Against Glow, Inc.* (Sep. 17, 2020), <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93>.
- ³⁷ Federal Trade Commission, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at 20 (2014), <https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014> (last visited Oct. 5, 2022) [hereinafter FTC DATA BROKER REPORT].
- ³⁸ To “dox” refers to the practice of publicizing online an individual’s real name (as opposed to screenname or handle), address, phone number, or other identifying information for the purposes of harassment. Often this information will be posted to a website encouraging other users to take action against the individual using that information. See Mat Honan, *What Is Doxing?*, WIRED (Mar. 6, 2014), <https://www.wired.com/2014/03/doxing/>.
- ³⁹ To “swat” refers to the practice of making a false but serious police report, such as alleging a hostage situation, to send law enforcement to the address of an innocent person for the purposes of harassing, embarrassing, and even injuring the target. See *The Crime of ‘Swatting’: Fake 9-1-1 Calls Have Real Consequences*, FBI.GOV NEWS (Sept. 3, 2013), <https://www.fbi.gov/news/stories/the-crime-of-swatting-fake-9-1-1-calls-have-real-consequences>.
- ⁴⁰ For instance, a Catholic priest was ousted from his position within the Church based on the work of a Catholic blog to link his previous location data with app data signals from the location-based hookup app Grindr. *Pillar Investigates: USCCB Gen Sec Burrill Resigns After Sexual Misconduct Allegations*, THE PILLAR (July 20, 2021), <https://www.pillaratholic.com/p/pillar-investigates-usccb-gen-sec>. See also Ylan Mui, *Little-Known Firms Tracking Data Used in Credit Scores*, Washington Post (July 16, 2011), https://www.washingtonpost.com/business/economy/little-known-firms-tracking-data-used-in-credit-scores/2011/05/24/gIQAXHeWII_story.html (describing how an Arkansas woman found her credit history and job prospects wrecked after she was mistakenly listed as a methamphetamine dealer; it took her years to clear her name and find a job).
- ⁴¹ *Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers*, FORBES (Sept. 7, 2017), <https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/>; See also It’s estimated that the entire data broker industry generates over \$200 billion in revenue every year. *What Are Data Brokers & How Do They Sell Your Identity?* (idshield.com). See Also Over 500 data brokers have registered with CA Attorney General: [Data Broker Registry | State of California - Department of Justice - Office of the Attorney General](#)
- ⁴² See Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELECTRONIC FRONTIER FOUNDATION (Dec. 2, 2019), <https://www EFF.org/wp/behind-the-one-way-mirror>.
- ⁴³ Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, Vox (July 8, 2020), <https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location>.
- ⁴⁴ See *What Are Cookies?*, CODE INSTITUTE, <https://codeinstitute.net/global/blog/what-are-cookies/> (last visited Oct. 5, 2022).
- ⁴⁵ See FTC DATA BROKER REPORT, *supra* note 37, at 29.
- ⁴⁶ Kevin Mellet & Thomas Beauvisage, *Cookie Monsters. Anatomy of a Digital Market Infrastructure*, 23 CONSUMPTION MKTS. & CULTURE 110, 110-129 (2020).
- ⁴⁷ Morey et al., *supra* note 1. Websites serving European audiences now feature cookie banners that purportedly notify consumers of the websites tracking practices. But researchers have found that majority of the policies still either lack information required by the GDPR (e.g., contact information for users to file privacy inquiries) or do not provide this information in a user-friendly form. Michael Kretschmer et al., *Cookie Banners and Privacy Policies: Measuring the Impact of the GDPR on the Web*, 15 ACM Transactions on the Web 1, 1-42 (2021).
- ⁴⁸ Kevin Sung et al., *Re-identification of Mobile Devices Using Real-Time Bidding Advertising Networks*, MobiCom ’20 1, 1-13 (2020).

-
- ⁴⁹ “Scientists ... had devised a computer algorithm that can identify 99.98 percent of Americans from almost any available data set with as few as 15 attributes, such as gender, ZIP code or marital status.” Gina Kolata, *Your Data Were ‘Anonymized’? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), <https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html> (citing Luc Rocher, Julien Hendrickx & Yves-Alexandre de Montjoye, *Estimating the Success of Re-identifications in Incomplete Datasets Using Generative Models*, 10 NAT COMMUN 3069 (2019), <https://www.nature.com/articles/s41467-019-10933-3>).
- ⁵⁰ This is driven in part by both Google’s and Apple’s decisions to prohibit some of these practices on their browsers or platforms. See David Temkin, *Charting a Course Towards a More Privacy-First Web*, GOOGLE: ADS & COMMERCE BLOG (Mar. 3, 2021), <https://blog.google/products/ads-commerce/a-more-privacy-first-web/>; Nick Statt, *Apple Updates Safari’s Anti-Tracking Tech with Full Third-Party Cookie Blocking*, THE VERGE (Mar. 24, 2020), <https://www.theverge.com/2020/3/24/21192830/apple-safari-intelligent-tracking-privacy-full-third-party-cookie-blocking>.
- ⁵¹ See PRIVACY SANDBOX, https://privacysandbox.com/intl/en_us/ (last visited Sept. 29, 2022).
- ⁵² Mark Gurman, *Apple Finds Its Next Big Business: Showing Ads on Your iPhone*, BLOOMBERG (Aug. 14, 2022), <https://www.bloomberg.com/news/newsletters/2022-08-14/apple-aapl-set-to-expand-advertising-bringing-ads-to-maps-tv-and-books-apps-l6tdqqmg>.
- ⁵³ Aleecia M. McDonald et al., *A Comparative Study of Online Privacy Policies and Formats*, in PROCEEDINGS OF THE 9TH INTERNATIONAL SYMPOSIUM ON PRIVACY ENHANCING TECHNOLOGIES 37, 42 (Ian Goldberg & Mikhail J. Atallah eds., 2009), available at <https://www.robreeder.com/pubs/PETS2009.pdf>.
- ⁵⁴ Florencia Marotta-Wurgler, *Understanding Privacy Policies: Content, Self-Regulation, and Markets* 31 (N.Y.U. L. & Econ., Research Paper No. 16-18, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736513.
- ⁵⁵ *Id.*
- ⁵⁶ F.T.C., BRINGING DARK PATTERNS TO LIGHT 15 (Sept. 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/P214800%20Dark%20Patterns%20Report%209.14.2022%20-%20FINAL.pdf.
- ⁵⁷ See *supra* note 15; Colorado Privacy Act, S.B. 21-190, 73d Leg., 2021 Reg. Sess. (Colo. 2021) (to be codified in COLO. REV. STAT. Title 6-1-1301) (effective July 1, 2023), https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf
- ⁵⁸ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Art. 5, <https://gdpr-info.eu/art-5-gdpr/>.
- ⁵⁹ California Privacy Rights Act, *supra* note 15. Similar language also appears in the bipartisan draft federal privacy bill, the American Data Privacy and Protection Act. See American Data Privacy and Protection Act, H.R.8152, 117th Cong. (2022), <https://www.congress.gov/bill/117th-congress/house-bill/8152/text#toc-H2505DD6E75214E79A8CB1B2E0A7EDDCD>. California law provides a private cause of action. CAL. CIV. CODE § 1798.150. States differ in remedies available under their respective privacy statutes.
- ⁶⁰ California Consumer Privacy Act Regulations Proposed Regulations (Cal. 2022) (to be codified in CAL. CODE REGS. 11 § 7000 – 7304), https://cippa.ca.gov/meetings/materials/20221021_22_item3_modtext.pdf.
- ⁶¹ *Id.* § 7002(b).
- ⁶² Colorado Privacy Act (CPA) draft regulations Rule 6.08, 45 Col. Reg. 19, 320, 340 (Oct. 20, 2022), <https://www.sos.state.co.us/CCR/RegisterPdfContents.do?publicationDay=10/10/2022>.
- ⁶³ For instance, most consumers impacted by last year’s T-Mobile data breach were “former or prospective T-Mobile customers” whose compromised information included “first and last names, date of birth, SSN, and driver’s license/ID information.” See *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack*, T-MOBILE NEWSROOM: NETWORK (Aug. 27, 2021), <https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation>.
- ⁶⁴ Assurance of Discontinuance, EyeMed Vision Care LLC, Att’y Gen. of the State of N.Y. Assurance No. 21-017 (Jan. 18, 2022), https://ag.ny.gov/sites/default/files/eyemed_aod_-_final_-_fully_signed.pdf.
- ⁶⁵ *Id.*
- ⁶⁶ *Connecticut Co-Leads \$1.25 Million Multistate Settlement Over 2019 Carnival Cruise Line Data Beach*, OFF. OF THE ATT’Y GEN. OF CONN. (June 22, 2022), <https://portal.ct.gov/AG/Press-Releases/2022-Press-Releases/Connecticut-Announces-Settlement-Over-2019-Carnival-Cruise-Line-Data-Breach>.

⁶⁷ For example, many companies are turning to “data lakes,” essentially servers with little technical oversight or management intended to collect raw data for analysis and processing later. These data lakes can become “data swamps” when too much data is added to them without proper management and maintenance. See Research and Markets, *Global Data Lake Market Analysis Report 2022: Market Revenue for 2021, Estimates for 2022 and 2023, and CAGR Projections Through 2027*, YAHOO! FINANCE (Aug. 26, 2022), <https://finance.yahoo.com/news/global-data-lake-market-analysis-085800903.html>.

⁶⁸ Assurance of Voluntary Compliance, Residual Pumpkin Entity, LLC, Atty’s Gen. of Conn., Indiana, Kentucky, Michigan, New Jersey, New York & Oregon, ORS 20.140 (Dec. 11, 2020), https://www.doj.state.or.us/wp-content/uploads/2020/12/AVC_Cafepress_2020.pdf (emphasis added).

⁶⁹ Complaint, Residual Pumpkin Entity, LLC & PlanetArt, LLC, F.T.C. File No. 1923209 (June 23, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/CafePress-Complaint_0.pdf.