Brooklyn Law Review

Volume 87 | Issue 2 Article 6

2-16-2022

The Gatekeepers of Research: Why a Data Protection Authority Holds the Key to Research in the New York Privacy Acts

Eric B. Green

The Gatekeepers of Research

WHY A DATA PROTECTION AUTHORITY HOLDS THE KEY TO RESEARCH IN THE NEW YORK PRIVACY ACTS

INTRODUCTION

"[R]esearch that enlightens us about the human condition is too valuable to abandon."— Jane R. Bambauer[1]

Your smart watch knows your resting heart rate,[2] what time you go to bed,[3] and whether you missed a workout.[4] The camera that unlocks your smart phone knows what your face looks like, down to your unique combination of dimples and wrinkles.[5] The applications on your smart phone store your medical history and can calculate your predisposition and active risk factors for certain mental and physiological conditions.[6] Moreover, in the impending era of

---

[1] Jane R. Bambauer, *Privacy Versus Research in Big Data*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 433, 433 (2018).

[2] *New Study Show Popular Smart Watches Accurately Measure Rapid Heart Beat*, HEART RHYTHM SOC'Y (2018), https://www.hrsonline.org/news/press-releases/new-study-show-popular-smart-watches-accurately-measure-rapid-heart-beat [https://perma.cc/62LC-LLBZ].

[3] Tara Sklar & Mabel Crescioni, *Research Participants' Rights to Data Protection in the Era of Open Science*, 69 DEPAUL L. REV. 699, 703 (2020); *Do Sleep Trackers Really Work?*, JOHN HOPKINS MED. (2020), https://www.hopkinsmedicine.org/health/wellness-and-prevention/do-sleep-trackers-really-work [https://perma.cc/MMM6-KTJG].

[4] James Stables, *Apple Watch: Activity and Workout App Explored and Explained*, WAREABLE (Dec. 24, 2019), https://www.wareable.com/apple/apple-watch-activity-and-workout-app-explained-875 [https://perma.cc/DB38-JACF].

[5] Under ideal conditions, facial recognition systems and applications achieve high classification accuracy. William Crumpler, *How Accurate Are Facial Recognition Systems—and Why Does It Matter?*, CTR. FOR STRATEGIC & INT'L STUD. (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter#:~:text=In%20ideal%20conditions%2C%20facial%20recognition,Recognition%20Vendor%20Test%20(FRVT) [https://perma.cc/9WBW-QY2B]. In reality, there may be inconsistencies in error rates across varying demographic groups. Alex Najibi, *Racial Discrimination in Face Recognition Technology*, SITNBOSTON (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology [https://perma.cc/YX6T-6BBN].

[6] *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 26 (2016) ("Health scores already exist, and a 'body score' may someday be even more important than your credit score. Mobile medical apps and social networks offer powerful opportunities to find support, form communities, and address health issues. But they also offer unprecedented surveillance of health data, largely ungoverned by traditional health privacy laws (which focus on doctors, hospitals, and insurers)." (footnote

minimum-contact doctor's appointments,[7] biometric data is on-track to spread more quickly and voluntarily.[8]

Experts project that we are entering a global inflection point, prompted by the evolution of the Internet of Things (IoT), or the massive network of things and people that process data about human behavior and environments.[9] Humankind has already developed the requisite technology to facilitate, albeit to a limited extent for now, the self-monitoring of our own biometric data, with assistance from the major institutional conglomerates that store such data.[10] The pressing question of tomorrow will be how much data you, as an individual, and we, as a society, are willing to share with these entities in exchange for the prospect of expedited human progress in science, medicine, and technology.

The New York Privacy Act (NYPA) and the Biometric Privacy Act (BPA) (collectively, the NY Privacy Acts),[11] while

---

omitted)); Natasha Singer, *When Apps Get Your Medical Data, Your Privacy May Go With It*, N.Y. TIMES (Sept. 3, 2019), https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html [https://perma.cc/HBV3-7X44]. *See generally* Sandeep Ravindran, *Smartphone Science: Apps Test and Track Infectious Diseases*, 593 NATURE 302, 302–03 (2021) (explaining how smartphones are a valuable tool for monitoring pathogens and testing for infectious disease).

[7] Progressive doctors' offices like "Forward" are introducing a new level of convenience into routine visits. Forward's patients are able to download and use the Forward application, which stores health data from their appointments. Amanda Capritto, *What It's Like Inside the Doctor's Office of the Future*, CNET (May 23, 2019, 4:00 AM), https://www.cnet.com/health/3d-body-scans-and-touchscreen-medical-records-inside-the-doctors-office-of-the-future [https://perma.cc/ET36-2E74]. The Forward app is compatible with Apple Health and uploads information such as vitals, exercise history, and dietary habits to a team of nurse practitioners, who then reach out if the data warrants any concerns. *Id.*; *How It Works*, FORWARD, https://goforward.com/how-it-works [https://perma.cc/HH5R-NK4H].

[8] *See generally* POTOMAC INST. FOR POL'Y STUD., BIOMETRIC DATA PRIVACY IN THE DIGITAL AGE (2020) (finding that biometric data generation in the US is rapidly increasing, and that convenience makes biometric security methods preferable to alternatives for consumers, thereby contributing to that growth). Hereinafter, "biometric data" or "biometric information" in this note means "one or more distinguishing biological characteristic[s] of an individual." *See* Hannah Zimmerman, Comment, *The Data of You: Regulating Private Industry's Collection of Biometric Information*, 66 U. KAN. L. REV. 637, 640 (2018). Biometric characteristics include physiological characteristics, e.g., facial features, fingerprints, DNA, and behavioral characteristics, e.g., typing rhythm or sleeping patterns. *Id.* Biometric data stored in a database can be combined to form an algorithm of a person's unique biometric characteristics. *Id.* at 641.

[9] Jen Clark, *What Is the Internet of Things (IoT)?*, IBM BUS. OPERATIONS BLOG (Nov. 17, 2016), https://www.ibm.com/blogs/internet-of-things/what-is-the-iot [https://perma.cc/LZH2-TKXS].

[10] Devices and applications that allow users to self-monitor their own health data are widely available at relatively low prices. *See* Btihaj Ajana, *Digital Health and the Biopolitics of the Quantified Self*, DIGIT. HEALTH 2–3 (Feb. 1, 2017), https://journals.sagepub.com/doi/pdf/10.1177/2055207616689509 [https://perma.cc/MDX7-E5YF]. These devices enable the average person to effortlessly employ quantitative methods of analysis, similar to those found in doctors' offices and research labs. *See id.*

[11] New York Privacy Act, S.B. 220., 2021-2022 Reg. Sess. (2021) /Assemb. B. 680A, 2021-2022 Reg. Sess. (2021); Biometric Privacy Act, Assemb. B. 27, 2021-2022 Reg. Sess. (N.Y. 2021).

massive strides in the right direction towards data privacy, are insufficient solutions to a surmounting problem around personal data,[12] and more specifically biometric data.[13] Personal data, despite its sensitivity, is indispensable to ensuring the quality and reliability of scientific and technological research and clinical trials.[14] Nonetheless, in their current forms, the NY Privacy Acts hardly recognize the need to protect usage of collected biometric data for conducting research or promoting public health.[15] Further, the NY Privacy Acts should require the creation of a data protection authority to tame the inevitable rise in biometric data capture and to ensure enforcement of the NY Privacy Acts' novel and necessary provisions.[16] A refined version of such a data protection authority would be capable of overseeing the flow and security of such data. Notably, personal data processing is crucial to produce research databases and for biobanking,[17] and to advance research, including clinical research and translational research.[18]

A modern movement marked by the rising use of wearables and smart devices is occurring simultaneously with a shift in the role of the research participant.[19] Even further, the surge in use of this technology has produced a high degree of realized and unrealized benefits to the scientific and technological

---

[12] "Personal data" under the NYPA "means any data that is identified or could reasonably be linked, directly or indirectly, with a specific natural person, household, or device. Personal data does not include deidentified data." S.B. 6701/Assemb. B. 680A.

[13] "Biometric information" under the NYPA "means any personal data generated from the measurement or specific technological processing of an individual's biological, physical, or physiological characteristics, including fingerprints, voice prints, iris or retina scans, facial scans or templates, deoxyribonucleic acid (DNA) information, and gait." S.B. 6701/Assemb. B. 680A.

[14] Gauthier Chassang, *The Impact of the EU General Data Protection Regulation on Scientific Research*, ECANCER 709 (Mar. 1, 2017), https://doi.org/10.3332/ecancer.2017.709 [https://perma.cc/4CQN-SV4F].

[15] As discussed in Part III of this note, the NY Privacy Acts do not adequately protect usage of personal data and biometric information for research purposes, as they do not recognize the importance of "secondary processing," and they do not clearly define the boundaries of scientific and other types of research. A data protection authority could assist in such an arduous endeavor as interpreting and enforcing the NY Privacy Acts. *See infra* Part IV.

[16] *See* S.B. 6701/Assemb. B. 680A; Assemb. B. 27.

[17] Biobanking refers to the practice of "collecting, storing, and sharing biological materials and associated data for present and future scientific research." Carly Cha, *Global Genes, Local Concerns: Legal, Ethical, and Scientific Challenges in International Biobanking*, 52 N.Y.U. J. INT'L L. & POL. 975 (2020).

[18] Chassang, *supra* note 14, at 3.

[19] *See* Mabel Crescioni & Tara Sklar, *The Research Exemption Carve Out: Understanding Research Participants Rights Under GDPR and U.S. Data Privacy Laws*, 60 JURIMETRICS 125, 126–27 (2020). Hereinafter, "wearable(s)" in this note means "small electronic device[s] containing . . . sensors that are integrated into clothing or other accessories worn on the body, such as on a wristband, . . . headband, . . . contact lens[es], or glasses." Sklar & Crescioni, *supra* note 3, at 703–04. Many of these devices have an intricate system of sensors that track a wearer's movement, orientation, or altitude. *See id.*

research and clinical trial processes.[20] Compared to the "high failure rate" of the traditional clinical trial design,[21] using wearables may provide more expeditious and accurate results at a lower cost, and with a previously unimaginable level of convenience to the research participant.[22] The future is positioned to reveal more abstract and novel uses of biometric data, presenting more innovation, but burdened by the prospect of intrusion.[23] For example, multinational corporations like Apple[24] have begun to repurpose personal-use biometric data from wearables for extensive research in the study of cardiovascular disease and brain illnesses, such as Alzheimer's.[25]

---

[20] Specifically, for some devices, measurements can be taken in a natural environment in a period of twenty-four-hours and for an extended period of time. Sklar & Crescioni, *supra* note 3, at 704–05.

[21] NIH Director, Francis Collins, expressed the failure rate as exceeding 95 percent, and the average length of time "from target discovery to regulatory approval" as thirteen years. Sklar & Crescioni, *supra* note 3, at 705.

[22] *Id.* at 703–05. This type of conveniently captured clinical trial data (collected from wearables) can be analyzed to produce real-world evidence, providing wearers and researchers with insight into how a medication or treatment affects daily activities and quality of life. *Id.* at 704–05.

[23] Elon Musk's Neuralink Project, for illustration, uses unobtrusive, wearable neuro-technologies to actively monitor a wearer's performance in work settings. Hiroki Kotabe, *Merging with Machines: A Look at Emerging Neuroscience Technologies*, NEUROSCIENCE NEWS & RSCH. FROM TECH. NETWORKS (Oct. 22, 2019), https://www.technologynetworks.com/neuroscience/articles/merging-with-machines-a-look-at-emerging-neuroscience-technologies-324859 [https://perma.cc/26VR-T4Z5]. That information is fed into a brain machine interface (BMI) that adaptively tailors custom solutions to improve performance. *Id.* Musk is not alone in such ventures. Another team of innovators is designing an unobtrusive wearable device that provides a multimodality overview of brain activity at any moment in a wearer's everyday life. *Id.*

[24] Apple launched its Research application in the United States in November 2019. *Apple Launches Three Innovative Studies Today in the New Research App*, APPLE NEWSROOM (Nov. 14, 2019), https://www.apple.com/newsroom/2019/11/apple-launches-three-innovative-studies-today-in-the-new-research-app [https://perma.cc/3P4Z-SFDF]. The shortest study, focused on hearing health, runs for two years with an optional two-year extension. The longest study, focused on women's health, may last for more than a decade. Jonah Comstock, *Apple Rolls Out Research: One App for Three New Longitudinal Studies*, MOBIHEALTHNEWS (Nov. 14, 2019, 9:01 AM), https://www.mobihealthnews.com/news/north-america/apple-rolls-out-research-one-app-three-new-longitudinal-studies [https://perma.cc/RDF7-SUGT]. Notably, each study requires a "research ethics committee," mirroring data protection authorities mandated by the European Union's General Data Protection Regulation and the California Consumer Privacy Act. *Sensor & Usage Data & Privacy*, APPLE SUPPORT (Apr. 26, 2021), https://support.apple.com/en-us/HT212042 [https://perma.cc/79RN-CCTN]; *see infra* Parts II.A, IV.B.

[25] The three initial studies of the Apple Research application were the Apple Heart and Movement Study, the Apple Hearing Study, and the Apple Women's Health Study. *Apple Announces Three Groundbreaking Health Studies*, APPLE NEWSROOM (Sept. 10, 2019), https://www.apple.com/newsroom/2019/09/apple-announces-three-groundbreaking-health-studies [https://perma.cc/H3AZ-UNQL]; Apple has also partnered with Biogen for a study that aims to identify digital biomarkers that can serve as early indicators of illnesses like Alzheimer's. Benjamin Mayo, *Apple and Biogen Announce New Research Study to Investigate How Apple Watch Can Detect Declines in Cognitive Health*, 9TO5MAC (Jan. 11, 2021, 7:31 AM), https://9to5mac.com/2021/01/11/apple-watch-biogen-cognitive-health-study [https://perma.cc/7B9G-7DM6]. Another survey in the Heart and Movement Study released in 2020 aimed to provide insight into how COVID-19 changed "daily life." Michael Potuck, *Apple Research App Updated with COVID-19 Survey and New 'Speech in Noise' Test*, 9TO5MAC (June 2, 2020, 10:02 AM), https://9to5mac.com/2020/06/02/apple-research-app-update [https://perma.cc/925N-SHMZ].

Further, national corporations have selected certain cities as pilot testing sites for new applications of biometric-facilitated transactions, such as finger-scan technologies at grocery stores.[26]

A small number of privacy acts, including the European Union's General Data Protection Regulation (GDPR),[27] the California Consumer Privacy Act (CCPA),[28] and the California Privacy Rights Act (CPRA),[29] already recognize the necessity to balance product users' privacy interests with expedited scientific progress and technological innovation.[30] These acts strive to achieve this balance by exempting data used for certain research from regulation, while also implementing "data protection authorities," or review boards that are simultaneously responsible for interpreting and enforcing the privacy acts.[31] In light of this balance, the GDPR has been widely praised for

---

[26] Amazon has instituted its palm-reading payment technology in NYC. Jon Fingas, *Amazon's Palm-Reading Payment Tech Is Now Available in New York City*, ENGADGET (May 10, 2021), https://www.engadget.com/amazon-one-palm-payment-new-york-city-130536589.html [https://perma.cc/E6D4-WKEH]. Moreover, a class action lawsuit was filed against Manhattan-based company, Clearview AI, to enjoin its alleged "'illegal[ ]' harvesting [of] people's photos from social media" and its infringement on the privacy of "nearly everyone in the United States." Dean Balsamini, *NYC Facial-Recognition Software Company Sued over Privacy, Civil Liberties Issues*, N.Y. POST (May 16, 2020, 5:47 PM), https://nypost.com/2020/05/16/clearview-ai-sued-over-privacy-civil-liberties-issues [https://perma.cc/D926-8M8M]. Some New York City Police Department officers have reportedly used Clearview AI for surveillance on their personal cell phones. *Id.*

[27] 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), 2016 O.J. (L 119) 1 [hereinafter GDPR].

[28] California Consumer Privacy Act of 2018, CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020).

[29] The California Privacy Rights Act serves to augment the existing CCPA and introduces a California Privacy Protection Agency to replace the state Attorney General's office as the regulator and enforcer of the California data privacy acts. California Privacy Rights Act of 2020, Proposition 24, *in* TEXT OF PROPOSED LAWS, CALIFORNIA GENERAL ELECTION VOTERS INFORMATION GUIDE 42–75 (Nov. 3, 2020) [hereinafter CPRA, Prop. 24], https://vig.cdn.sos.ca.gov/2020/general/pdf/topl.pdf [https://perma.cc/S8NC-YSA7] (approved on Nov. 3, 2020, operative Jan. 1, 2023); Liisa M. Thomas et al., *The CCPA Wheels Keep Turning: The Addition of CPRA*, NAT'L L. REV. (Nov. 5, 2020), https://www.natlawreview.com/article/ccpa-wheels-keep-turning-addition-cpra [https://perma.cc/5ZLA-EHGA].

[30] Ethical standards for research involving biometrics recognize a balance between the "societal need for scientific development" and individual privacy and autonomy. Ciara Staunton et al., *The GDPR and the Research Exemption: Considerations on the Necessary Safeguards for Research Biobanks*, 27 EUR. J. HUM. GENETICS 1159, 1160 (2019). "The Taipei declaration states that '[r]esearch should pursue science advancement and public health development while respecting the dignity, autonomy, privacy and confidentiality of individuals.'" *Id.* (alteration in original).

[31] Hereinafter, a "data protection authority" in this note means an "independent public authorit[y] that monitor[s] and supervise[s] the application of [their respective region's] data protection law [or laws]." *What Are Data Protection Authorities (DPAs)?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-are-data-protection-authorities-dpas_en [https://perma.cc/2HEA-9UTR]. Data protection authorities are discussed in Parts II and IV of this note.

"raising the bar" for comprehensive data privacy regimes,[32] and the CCPA and CPRA have positioned themselves as the GDPR's American equivalents.[33]

A federal biometrics privacy statute is not on the horizon, despite the fact that it should be.[34] Thus, the torch has been passed to states. Recognizing the unlikelihood of a federal statute and the increased use of biometric data processing and storage, states like Illinois, California, Washington,[35] and Texas[36] have taken it upon themselves to light their own respective torches and create their own protective regimes.[37]

For illustration and comparison, Illinois is commonly hailed as the first state to enact a comprehensive biometrics privacy act:[38] the Biometrics Information Privacy Act (BIPA).[39] Before listing all of BIPA's restrictions and prohibitions in the text, BIPA's drafters expressly recognized the uniquely sensitive

---

[32] Giovanni Buttarelli, *The EU GDPR as a Clarion Call for a New Global Digital Gold Standard*, EUR. DATA PROT. SUPERVISOR (Apr. 1, 2016), https://edps.europa.eu/press-publications/press-news/blog/eu-gdpr-clarion-call-new-global-digital-gold-standard_de [https://perma.cc/B4JD-L659].

[33] *See Data Privacy and Compliance in 2021: CCPA, CPRA,GDPR*, SPIRION (Feb. 4, 2021), https://www.spirion.com/blog/data-privacy-compliance-ccpa-cpra-gdpr [https://perma.cc/2HJV-YYN5].

[34] "There is no single principal data protection legislation in the United States." F. Paul Pittman & Kyle Levenberg, *Data Protection 2020*, GLOB. LEGAL GRP. (June 7, 2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa [https://perma.cc/6TUE-4F56]; "America's patchwork of weak privacy laws are no match for the threats posed by this runaway data, which is used to secretly rank, rate, and evaluate persons, often to their detriment and often unfairly." PASQUALE, *supra* note 6, at 21.

[35] The Washington Privacy Act, S.B. 6281, 2019-2020 Reg. Sess. (Wash. 2019), would have given Washington residents the right to access, correct, or delete data stored and processed on them by commercial entities. Cathy Cosgrove, *The Washington Privacy Act Is Back*, IAPP (Sept. 23, 2020), https://iapp.org/news/a/the-washington-privacy-act-is-back [https://perma.cc/S4PB-7ZK2]. The Senate's version would have granted enforcement authority to the state attorney general, whereas the House's version granted citizens a private right of action. *Id.* The Washington Senate and House failed to reach a consensus in 2020, and the Senate subsequently released a new draft bill for consideration in 2021. *Id.*

[36] The Texas Capture or Use of Biometric Identifier Act (CUBI) applies to the collection of biometric information for commercial purposes and imposes similar obligations, such as the destruction of biometric data. Jeffrey N. Rosenthal et al., *Meet CUBI—What Companies Need to Know About Texas' Biometric Privacy Law*, LAW.COM (Oct. 5, 2020, 11:41 AM), https://www.law.com/texaslawyer/2020/10/05/meet-cubi-what-companies-need-to-know-about-texas-biometric-privacy-law [https://perma.cc/U96D-XCRP]. CUBI also imposes a conditional prohibition on profiting from biometric information. *Id.*

[37] Compared to the privacy acts of Washington and Texas, California's acts have been passed into law, are sufficiently comprehensive, and include data protection authorities. Thus, California's CCPA and CPRA are focal points of this note and discussed in Part II.

[38] The first comprehensive state biometric privacy legislation, Illinois's Biometrics Information Privacy Act, became effective in October 2008. Quinn, Emanuel, Urquhart & Sullivan, LLP, *June 2019: The Rise of Biometrics Laws and Litigation*, JD SUPRA (June 28, 2019), https://www.jdsupra.com/legalnews/june-2019-the-rise-of-biometrics-laws-82168 [https://perma.cc/U3PL-R8VS].

[39] Biometric Information Privacy Act, 740 ILL. COMP. STAT. 14 (2018).

nature of biometric data.[40] BIPA ultimately creates a broad security requirement: private entities in possession of biometric data must use "reasonable," industry-specific standards of care.[41] As a direct result of these obligations, combined with BIPA's private right of action,[42] Illinois courts have seen a sharp increase in litigation.[43]

New York is another state that shows promise in the area of personal data protection. New York has a number of tabled consumer privacy bills, including the NYPA, the Right to Know Act,[44] and the It's Your Data Act.[45] However, to the detriment of New Yorkers, the New York legislature has not passed any of these bills.[46] The NYPA purports to grant New Yorkers certain rights, including the right to erasure,[47] arising from third-parties' storage of personal

---

[40] *Id.* at 14/5(c) ("Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions."). From the outset, BIPA also notes that public welfare and security are bolstered by close regulation of the "collection, use, safeguarding, handling, storage, retention, and destruction" of biometric information. *Id.* at 14/5(g).

[41] BIPA imposes on private entities a number of distinct obligations, including a broad prohibition on profiting from biometric data, and a limited prohibition on disclosing biometric information barring explicit consent for a singular and necessary purpose. *Id.* at 14/15. Further obligations imposed by BIPA include, but are not limited to, (1) requiring private entities in possession of biometric data to develop and make public a written policy "establishing a retention schedule and guidelines for" permanent destruction of biometric data; and (2) prohibiting private entities from obtaining biometric data without informed written consent. *Id.* at 14/15(e)(1–2); Lydia de la Torre et al., *The Illinois Biometric Information Privacy Act ("BIPA"): When Will Companies Heed the Warning Signs?*, NAT'L L. REV. (Feb. 17, 2020), https://www.natlawreview.com/article/illinois-biometric-information-privacy-act-bipa-when-will-companies-heed-warning [https://perma.cc/S62M-R5RU].

[42] BIPA's private right of action enables aggrieved persons to recover "for each violation" liquidated damages of upwards of $5,000 or actual damages (whichever is greater). 740 ILL. COMP. STAT. 14/20(2).

[43] Following the Illinois Supreme Court's ruling in *Rosenbach v. Six Flags Entertainment Corporation*, 129 N.E.3d 1197, 1207 (Ill. 2019), consumers have standing to sue under BIPA. de la Torre et al., *supra* note 41.

[44] The Right to Know Act of 2021 would require businesses to provide their customers with access to their personal information disclosed to third parties, and the names and contact information of all such third parties. Assemb. B. 400, 2021-2022 Reg. Sess. (N.Y. 2021). This is similar to requirements under California's Shine the Light law. Cal. Civ. Code § 1798.83 (West 2020).

[45] The It's Your Data Act, in addition to imposing civil liabilities, would impose criminal liabilities on any person, firm, or corporation that collects, stores, or uses for commercial purposes the personal data of any living person without their consent. Assemb. B. 3586, 2021-2022 Reg. Sess. (N.Y. 2021)/S.B. 4021, 2021-2022 Reg. Sess. (N.Y. 2021).

[46] The New York Privacy Act, the Right to Know Act, and the It's Your Data Act have not passed either house of the New York State Legislature. *See NY A00680*, BILL TRACK 50, https://www.billtrack50.com/billdetail/1255827 [https://perma.cc/5TSE-JG92]; *NY A00400*, BILL TRACK 50, https://www.billtrack50.com/billdetail/1254439 [https://perma.cc/B2D5-Z3JM]; *NY A03586*, BILL TRACK 50, https://www.billtrack50.com/billdetail/1291995/ [https://perma.cc/6FX5-NS5Y].

[47] New York Privacy Act, S.B. 6701, 2021-2022 Reg. Sess. (2021)/Assemb. B. 680A, 2021-2022 Reg. Sess. (2021). Hereinafter, the "right to erasure" in this note means the allowance for people to request that their personal data, generally commercial data, be erased.

data.[48] The NYPA is novel in its creation of an "opt-in" regime for processing data, such that consumers would need to explicitly consent to have their data collected.[49]

In January 2021, bipartisan New York legislators proposed the BPA.[50] The BPA would require entities to obtain explicit consumer consent before collecting, capturing, purchasing, trading, or storing biometric information or identifiers.[51] Mirroring Illinois's BIPA, consumers would have a private right of action to enforce BPA violations.[52] The provisions of the BPA would complement those under the NYPA, filling the apertures through which violations in biometric data protection would otherwise pass.

This note argues that, by more clearly defining the research exemption to the erasure of biometric data and by mandating the imposition of data protection authorities, the pending NY Privacy Acts can compete with the GDPR, CCPA, and CPRA in their scope of protections and the benefits they provide. Part I discusses the risks associated with biometric data exposure and the benefits of deidentifiable biometric data to research. It also includes a primer on methods of deidentification. Part II provides background on the GDPR, CCPA, and CPRA, contrasting the right of erasure, research

---

It is alternatively (and aptly) referenced, usually in the context of the GDPR, as the "right to be forgotten." Ben Wolford, *Everything You Need to Know About the "Right to Be Forgotten*," GDPR.EU, https://gdpr.eu/right-to-be-forgotten [https://perma.cc/LX93-GS5Y]. This right is particularly applicable where such data is "no longer necessary in relation to the purposes for which they were collected or otherwise processed." GDPR, *supra* note 27, art. 17, ¶ 1(a). In the absence of a clearly defined research exemption, data subjects may choose when to withdraw consent from retention of the data. *See* Wolford, *supra*.

[48] S.B. 6701/Assemb. B. 680A.

[49] Viola Trebicka et al., *Inside the Proposed New York Privacy Act*, LAW.COM (Sept. 2, 2020), https://www.law.com/newyorklawjournal/2020/09/02/inside-the-proposed-new-york-privacy-act/#:~:text=Opt%2DIn%20Requirement.&text=The%20%E2%80%9Copt%20in%E2%80%9D%20process%20requires,%C2%A71100(2) [https://perma.cc/H8HS-L6P6].

[50] Assemb. B. 27, 2021-2022 Reg. Sess. (N.Y. 2021).

[51] The BPA's definition of "biometric information" is "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." *Id.* Even still, the definition explicitly excludes "information derived from items or procedures excluded under the definition of biometric identifiers." *Id.* The list of exclusions under the definition of "biometric identifiers" is notably and significantly longer than the items that are included. *Id.*

[52] Under the language of the BPA, "[a]ny person aggrieved by a violation of this article shall have a right of action in supreme court against an offending party." *Id.* The BPA then sets forth the amounts an aggrieved person may recover from a private entity. For a negligent violation, the aggrieved may recover $1,000 or actual damages, whichever is greater. For an intentional or reckless violation, the aggrieved may recover $5,000 or actual damages, whichever is greater. *Id.* If the BPA will be broadly construed by courts in New York, as was BIPA by courts in Illinois in cases like *Rosenbach*, *see supra* note 43, the result may be a drastic increase in litigation as well as harm to businesses in New York and those that conduct business therein.

exemptions, and data protection authorities under each act. Part III introduces and describes the provisions of the NY Privacy Acts and explains their shortcomings in relation to similar provisions within the GDPR, CCPA, and CPRA. Part IV proposes and justifies a clear, tripartite definition and scope of scientific research and the research exemption, inspired by the GDPR, the CCPA, and the "open science" concept.[53] It further proposes that the legislature should amend the NY Privacy Acts to mandate the establishment of a data protection authority and a specialized biometrics subcommittee, empowered with the ability to interpret the legislation and ensure compliance.

I. THE DANGER (AND DANGEROUSLY APPEALING BENEFITS) OF BIOMETRIC DATA PROCESSING AND RELEVANT DEIDENTIFICATION CONSIDERATIONS

"Algorithms allow our devices and apps to run hundreds of little experiments a day."[54] Moreover, under the American Common Rule, which provides mandates for ethical research, data that has been deidentified can be shared and processed for research purposes.[55] Deidentification does not completely eliminate the risk that accompanies biometric data processing, but that risk pales in comparison to the immense benefits to society from being able to more freely share biometric data for research.[56]

A. The Risks and Benefits Associated with Biometric Data Processing

From a privacy perspective, biometric data is the most sensitive type of data because it is biologically tied and unique to the individual.[57] Unlike social security numbers, most biometric data markers cannot be changed once compromised.[58] Thus, when this data is compromised, the individual is left with no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.[59]

---

[53] Open science is the practical and theoretical proposition of making scientific research and its dissemination accessible to all levels of an inquiring society. See *infra* notes 69–71 for a discussion of the benefits of open science and secondary processing in easing the communication of scientific knowledge.

[54] Bambauer, *supra* note 1, at 435.

[55] *Id.* at 434–35.

[56] *Id.* at 442.

[57] 740 ILL. COMP. STAT. 14/5(c) (2018).

[58] *Id.*

[59] *Id.*

Typically, biometric data stored on wearables is uploaded to a smart device via a Bluetooth connection,[60] then transmitted to a server that holds a larger data set.[61] Businesses commonly adopt their own protocols about how personal data can be collected from wearables into third-party systems, but third-party server communication can result in security and privacy issues.[62] Commercial cloud storage systems, like Apple's iCloud storage system, encode each user's data with a specific encryption key.[63] Encryption results in data appearing scrambled and unreadable, requiring intruders to decode the key in order to access the personal information.[64] The timing of the encryption and where those keys are held—and therefore the extent of security therein—tends to vary based on the service provider.[65] Thus, in the absence of privacy legislation mandating a uniform process for biometric data collection, consumers face risk not only from the sale of their biometric data to third-parties for commercial benefit, but also by the improper storage of personal data.

Despite the clear and present dangers posed by biometric data collection, biometric data is an invaluable facet of the research that enables progressive scientific and technological innovation.[66] The benefits of biometric data usage are illustrative in the context of clinical trials, whereby vitals are necessary to track a medication's effectiveness.[67] Furthermore, it is common practice in scientific research for fully encrypted personal data to be used for a purpose separate from that of the initial processing.[68] This type of "secondary processing" is an essential ingredient for maximizing the accuracy and efficiency of scientific research.[69]

---

[60] "A smart device is an electronic device, generally connected to other devices or networks via different protocols such as Bluetooth, NFC, WiFi, 3G, etc., that can operate to some extent interactively and autonomously." *What Is Smart Device*, IGI-GLOB., https://www.igi-global.com/dictionary/smart-device/47498 [https://perma.cc/QQY7-YFEB].

[61] Francisco de Arriba-Pérez et al., *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios*, SENSORS (Sept. 21, 2016), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5038811 [https://perma.cc/MDP4-FWTX].

[62] *Id.*

[63] Haibin Zhang, *How Secure Is Your Data When It's Stored in the Cloud?*, SCI. AM. (Jan. 25, 2018), https://www.scientificamerican.com/article/how-secure-is-your-data-when-it-rsquo-s-stored-in-the-cloud/#:~:text=Data%20stored%20in%20the%20cloud,varies%20among%20cloud%20storage%20services [https://perma.cc/WU3W-JB77].

[64] *Id.*

[65] *Id.*

[66] Benefits to using wearables in clinical trials, for example, would reduce barriers, lower costs, and accelerate the regulatory approval process, with results that could substantially benefit public health. *See* Sklar & Crescioni, *supra* note 3, at 704–08.

[67] Chassang, *supra* note 14.

[68] *Id.*

[69] Hereinafter, "secondary processing" will refer to any and all future uses of the same deidentifiable data, not limited to one single use. Secondary processing has the essential role of preserving time and resources for researchers. *Id.*

The purposes surrounding secondary processing are similar to those of the "open science" movement. Open science is the practical and theoretical proposition of making scientific research and its dissemination accessible to all levels of an inquiring society, amateur or professional.[70] Its central focus is on the transparency, reproducibility, and availability of scientific products and output, to allow knowledge and data to be shared and developed through collaborative networks.[71] Admittedly, extending access to sensitive information to all of society seems to tip the scales towards more risk than benefit. Still, the notion should be considered in humanity's reevaluation of biometric data usage in the years to come, at least in part and as it relates to communities of professionals.

B. A Primer on Deidentification Requirements and Methods

Generally, if an entity can prove that the identity of an individual cannot be derived from anonymized data, then the data may be exempt from other security methods.[72] In other words, processes exist that reconstruct personal, identifiable data into data that cannot be traced back to the individual. When an entity uses one of these processes and proves that the process is successful, the entity may be exempt from certain security or privacy requirements, such as required recognition of an individual's right to erasure.[73] Thus, the GDPR, the CCPA, and the CPRA require entities that process personal data to deidentify that data through pseudonymization,[74] anonymization,[75] and other similar methods of

---

[70] *See* Sean Granta & Kathryn E. Bouskill, Opinion, *Why Institutional Review Boards Should Have a Role in the Open Science Movement*, 116 PNAS 21336, 21336 (2019).

[71] *See id.* at 21336–37. "Open science" includes practices such as encouragement of open-notebook science (material and data sharing) and publication of summary findings in open access outlets, which generally make it easier to publish and communicate scientific knowledge. *Id.*

[72] *Data Masking: Anonymisation or Pseudonymisation?*, GRC WORLD FORUMS, https://gdpr.report/news/2017/11/07/data-masking-anonymisation-pseudonymisation [https://perma.cc/TDF9-63ZM].

[73] *Id.*

[74] "Pseudonymization" in this note means the process of enhancing privacy by replacing identifying characteristics (e.g., a social security number) in a data set with artificial identifiers, aliases, or pseudonyms. Pseudonymization more generally "is a reversible process that de-identifies data but allows the reidentification later on if necessary." *Pseudonymization According to the GDPR [Definitions and Examples]*, DATA PRIVACY MANAGER (May 2, 2021), https://dataprivacymanager.net/pseudonymization-according-to-the-gdpr [https://perma.cc/SG5C-2MZN]. After defining "pseudonymized," the CCPA only refers to the term once. *What Is 'Pseudonymized' Data?*, BCLP L. (Jan. 17, 2020), https://www.bclplaw.com/en-US/insights/what-is-pseudonymized-data.html [https://perma.cc/XZ8C-YVAU] ("Within the definition of 'research,' the CCPA implies that personal information collected by a business should be 'pseudonymized and deidentified' or 'deidentified and in the aggregate.'" (quoting CAL. CIV. CODE 1798.140(s)(2)).

[75] "Anonymization," unlike pseudonymization, scrubs all information from the data that may be used to reidentify a data subject. *See Pseudonymization According to*

concealing personal data.[76] Amendments to the CCPA suggest even clearer rules for deidentification by employing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule deidentification methods,[77] including the Expert Determination method and the Safe Harbor method.[78] The purposes of both methods are to prevent reidentification of any given individual and the reversal of any deidentification techniques.[79]

New methods of biometric and other personal data encryptions provide motivational triggers for society to reconsider data's valuable role in scientific and medical research. For example, a newly developed technology called fully homomorphic encryption (FHE) exceeds current federal and state law standards meant to safely protect biometric data.[80] FHE is capable of surviving intrusion attempts—even by future quantum computers yet to be developed—rebutting the assertion that new security methods will always be undermined by new methods of exposition.[81] FHE is among the methods of encryption that completely conceal the source of data without sacrificing the data's utility.[82]

---

the GDPR [Definitions and Examples], *supra* note 74. If the data is anonymized so the data subject is no longer identifiable (directly or indirectly), statutes like the GDPR may no longer consider it as personal data. *Id.*

[76] *See* GDPR, *supra* note 27, arts. 9, 89 (prohibiting the processing of personal data for the purpose of uniquely identifying a natural person and requiring measures such as pseudonymization for derogations to restrictions); CCPA, CAL. CIV. CODE §§ 1798.100–1798.199 (West 2020) (similarly requiring methods of deidentification for research and for derogations to restrictions).

[77] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of Titles 18, 26, 29 and 42 of the United States Code).

[78] The Expert Determination method involves the transfer of the data to a person or entity skilled in the application of statistical disclosure techniques who then deidentifies the data, with the resulting very small risk that anticipated recipients could identify a given individual. 45 C.F.R. § 164.514 (b)(1); *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, HHS.GOV (Nov. 6, 2015) [hereinafter *HIPAA Privacy Rule Guidance*], https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#_edn1 [https://perma.cc/QR6B-YCDD]. The Safe Harbor method involves the removal of eighteen types of identifiers, resulting in no actual knowledge of residual information that can identify a given individual. *See* 45 C.F.R. § 164.514(b)(2); *HIPAA Privacy Rule Guidance*, *supra* note 75.

[79] *HIPAA Privacy Rule Guidance*, *supra* note 78.

[80] Dario Gil, *How to Preserve the Privacy of Your Genomic Data*, SCI. AM. (Nov. 9, 2020), https://www.scientificamerican.com/article/how-to-preserve-the-privacy-of-your-genomic-data/#:~:text=Preserving%20genomic%20privacy%20is%20just,medical%20records%20or%20financial%20information [https://perma.cc/898D-5DLV].

[81] *Id.*

[82] Contrary to less successful methods, the data in use remains "cryptographically jumbled" to ensure privacy while it is being processed; even the handlers of the data are unable to uncover the data set's contents. *Id.*

II. A CHAIN OF INSPIRATION: THE GDPR, THE CCPA, AND THE CPRA

As a threshold matter, the GDPR reflects the European Union's preference for a comprehensive privacy regime,[83] whereas the United States' patchwork of federal privacy laws reflects its preference for a sectoral regime, or one that is focused on industry-specific legislation.[84] The increase in state-specific privacy legislation adds an additional layer of privacy considerations for entities that process data for research. Nonetheless, the CCPA and CPRA share many features of the GDPR and can serve as helpful anchors from which to critique the NY Privacy Acts.

A. Comparing Rights to Erasure, Research Exemptions, and Data Protection Authorities

While the GDPR, CCPA, and CPRA differ in the intensity of their privacy protections, they offer the same types of protections as the NY Privacy Acts. This Section discusses how each act defines (1) the right to erasure, (2) the research exemption, and (3) the mandated or recommended implementation of a data protection authority.[85]

1. Right to Erasure: GDPR and CCPA

The GDPR was the first major comprehensive privacy act to establish an individual's right to erasure for all data, including biometric data.[86] Under Article 17 of the GDPR, individuals have the right to have personal data erased.[87] For reference, the GDPR defines personal data as "any information relating to an identified or identifiable natural person."[88]

The GDPR's right to erasure is not absolute.[89] For example, and for the purposes most relevant to this note, the right to erasure may not apply "for archiving purposes in the public interest, scientific or historical research purposes or

---

[83] PETER SWIRE & DEBRAE KENNEDY-MAYO, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 19 (3d ed. 2020).

[84] *Id.* at 21.

[85] *What Are Data Protection Authorities (DPAs)?*, *supra* note 31.

[86] *See* GDPR, *supra* note 27, art. 17, ¶ 1 (creating a right to erasure or "right to be forgotten" of an individual's personal data at their request if one or more of a number of factors are applicable).

[87] *Id.*

[88] *Id.* art. 4, ¶ 1.

[89] Article 89 provides safeguards and derogations relating to processing of data for public interest purposes or, scientific, historical, or statistical research purposes. *Id.* art. 89, ¶ 1. Article 17 also lists categories whereby an exemption would apply. *Id.* art. 17, ¶ 1.

statistical purposes" where erasure is likely to render impossible or seriously impair the achievement of that processing.[90] Further, the GDPR explicitly states that the right to erasure will not apply if the processing is necessary for public health purposes that are "in the public interest."[91] The GDPR research exemption continues to influence state privacy laws and has the potential to influence future federal privacy law as well.[92]

The CCPA also contains a right to erasure.[93] This right allows California consumers to request that businesses and service providers erase their personal information.[94] Consumers can exercise this right if the business or service provider (1) collected the personal information from the consumer, (2) no longer needs to maintain the personal information,[95] and (3) is not entitled to retain such information.[96] This right carries with it certain ambiguities, principally because the CCPA does not define the term "delete" or outline when data retention would no longer be necessary.[97]

2. Research Exemptions: GDPR, CCPA, and CPRA

The concept of scientific research in the GDPR is introduced at Recital 159, which explains that personal data processed for scientific research purposes is also subject to provisions of the GDPR.[98] However, various articles create exemptions related to scientific research that limit certain rights of consumers.[99] Of particular relevance to this note are Article 17, providing an exemption from the right to erasure for personal data used for scientific research, and Article 89, identifying scientific research and the public interest as triggers

---

[90] *Id.* art. 89, ¶ 1.

[91] Examples include protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices. *Id.* at recital 53.

[92] Bart Van den Brande, *Data Protection Laws Inspired by GDPR Are Spreading Across the World. Is New York Next?*, SIRUIS.LEGAL (Sept. 12, 2019), https://www.lexology.com/library/detail.aspx?g=0a3d251c-bdae-479a-a29f-7fb1988c1f03 [https://perma.cc/2Z3G-2ED3].

[93] CAL. CIV. CODE § 1798.105(a) (West 2020).

[94] *Id.* The CCPA defines personal information broadly to include "information that [can] identif[y], relate[ ] to, describe[ ]," be associated with, or be "reasonably capable of being associated with . . . a particular consumer or household." *Id.* § 1798.140(o)(1).

[95] *Id.* § 1798.105(a), (d).

[96] This is permissible through one of the general exemptions under CAL. CIV. CODE § 1798.145.

[97] *Consumer Rights and Information: FAQs*, BCLP L., https://ccpa-info.com/faqs/consumer-rights-and-information-faqs [https://perma.cc/QQ4U-JVXJ].

[98] GDPR, *supra* note 27, at recital 159.

[99] *Id.* art. 17, ¶ 3; art. 89 ¶¶ 2–3.

to potential exemptions of other rights,[100] which European Union Member States can choose to implement.[101]

Importantly, the GDPR contains neither a formal definition nor a formally defined scope of what constitutes scientific research.[102] Instead, the law prescribes that processing of personal data for scientific research purposes should be interpreted "in a broad manner."[103] Recital 159 lists examples, including "technological development and demonstration, fundamental research, applied research and privately funded research . . . studies conducted in the public interest in the area of public health."[104]

One problematic scenario arises as a result of the GDPR's failure to sufficiently consider the long-standing industry-specific ethical standards of research currently in place.[105] This gap between data privacy law and existing standards leads to confusion in application.[106] Another problem with the lack of a defined scope of "research" arises from the principle of "purpose limitation[s],"[107] such as the distinction between collecting data for the purpose of scientific research versus for the purpose of statistical research.[108] While, as noted above, the GDPR does not define scientific research, the informal and commonly applied definition is "any activity aimed at generating new knowledge and advancing the state of the art in a given field."[109] Statistical research, on the other hand, is "the processing of personal data . . . for statistical surveys or . . . results," including those used in support of scientific research.[110] The GDPR states that statistical research can be

---

[100] *Id.* art. 89 ¶¶ 2–3. Article 89 provides that, "where personal data is processed for scientific or historical research purposes or statistical purposes," Member State law may allow for exemptions to the right of access, *see id.* art. 15; right to rectification, *see id.* art. 16; right to restriction of processing, *see id.* art. 18; and right to object to processing, *see id.* art. 21.

[101] *Id.* art. 89 ¶¶ 2–3.

[102] Rossana Ducato, *Data Protection, Scientific Research, and the Role of Information*, 37 COMPUT. L. & SEC. REV. 2, 3 (2020).

[103] GDPR, *supra* note 27, at recital 159.

[104] *Id.*

[105] Data privacy legislation may conflict with current ethical standards, international treaties and other legal instruments, making the exemption process more challenging. *See* Staunton et al., *supra* note 30, at 1159–60. For example, researchers in the area of health and science have been guided by the World Medical Association's Declaration of Helenski and Taipei Declation, which deviate from provisions of the GDPR. *Id.* at 1162–63.

[106] *See id*. at 1159–60.

[107] A "purpose limitation" is the requirement that personal data be collected for specific purposes, and that it not be processed for other purposes. GDPR, *supra* note 27, art. 5(1)(b).

[108] Ducato, *supra* note 102, at 2–3.

[109] *Id.* at 3. Scientific research encompasses activities for profit, e.g., research and development efforts by a company "to improve or offer new services." *Id.*

[110] GDPR, *supra* note 27, at recital 162 (defining statistical purposes as "any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results").

reused for other purposes to maximize the utility of the data, including further processing for scientific research purposes, but it notes that statistical purposes themselves do not include scientific research.[111] The cryptic and overlapping descriptions of purpose limitations prompt confusion in application, ultimately having negative effects on scientific research.[112]

Much like the GDPR, the CCPA identifies a few situations where a business or a service provider is not required to comply with a consumer's request to delete personal information.[113] Notably, a business may deny a request to delete where retaining the information is necessary for the business or service provider to perform a contract between the business and the consumer.[114] In addition, a business may also deny a request when it is using the data for "public or peer-reviewed scientific, historical, or statistical research in the public interest . . . [if] deletion of the information is likely to render impossible or seriously impair the achievement of such research."[115] Research under the CCPA is defined as "scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health."[116]

The California legislature initially neglected to include exemptions for clinical trials, but later amended the CCPA to include the exemption.[117] The amendment clarified that the research exemption applies to personal data collected for research conducted in accordance with the HIPAA Privacy Rule, which defines research broadly as "a systemic investigation, including research development, testing, evaluation, designed to develop or contribute to generalizable knowledge."[118] The California legislature currently labels personal data for clinical trials and other biomedical research studies as being subject to potential exemptions.[119]

---

[111] *Id.*

[112] The possibility of applying a statistical result to a particular person is not covered by the law. If processing has consequences at the individual level, data controllers cannot benefit from the "favorable" regime under Article 89. Ducato, *supra* note 102, at 4.

[113] CAL. CIV. CODE § 1798.105(d) (West 2020).

[114] *Id.*

[115] *Id.* § 1798.105(d)(6).

[116] *Id.* § 1798.140(s).

[117] Christian M. Auty, *Implications of CCPA and CPRA on Clinical Trial Data*, BCLP L. (Oct. 21, 2020), https://www.bclplaw.com/en-US/insights/implications-of-ccpa-and-cpra-on-clinical-trial-data.html [https://perma.cc/HT2D-YCPH] (noting that the CCPA amendment was approved by California's governor on September 25, 2020).

[118] *Id.* 45 C.F.R. § 164.501.

[119] These exemptions are applicable so long as the data used is not sold and as participants are informed of and consent to such use. *Id.* Notably, "clinical trials" and "biomedical research" remain undefined. *Id.*

The amendment has already been implemented,[120] but the exemption will prove intractable for the majority of businesses to use in practice, quelling some fears arising from the commercial sale of biometric data.[121] First, the research to which the exception applies must be public, peer-reviewed, and in the public interest.[122] In addition, the definition of research provides that the work or study shall "[n]ot be used for any commercial purpose."[123] It is difficult—but not impossible—to imagine a scenario where a business conducts research in the public interest that does not simultaneously advance the business's commercial or economic interests.[124]

A major problem arose in California following the enactment of the CCPA regarding the boundaries of the term "research," mirroring the European Union's problems created by the GDPR.[125] The CCPA left unresolved the scope of its application to data processed for research in the fields of science and medicine.[126] Specifically, CCPA exemptions failed to address industry-wide frameworks and regulations, such as HIPAA, used for scientific and medical research and clinical trials.[127] As a result, California legislators proposed an amendment to the CCPA to reconcile the CCPA with the deidentification standards set forth in HIPAA, and to provide other important clarifications for researchers.[128] The legislators deemed the negative effects on research to be sufficiently pressing so as to render the bill an "urgency statute."[129] These effects are particularly harmful in the

---

[120] Alex Nisenbaum & Karen Shin, *AB-713 CCPA Requirements Take Effect January 1, 2021 for Use of De-identified Health Data Sets*, JD SUPRA (Dec. 10, 2020), https://www.jdsupra.com/legalnews/ab-713-ccpa-requirements-take-effect-42027 [https://perma.cc/756J-LFTX].

[121] Gregory A. Gidus, *The Research Exception to the CCPA's Right to Deletion—Will It Ever Apply?*, CARLTON FIELDS (July 17, 2019), https://www.carltonfields.com/insights/publications/2019/research-exception-ccpa-right-deletion-apply [https://perma.cc/4JQ3-46K7].

[122] CAL. CIV. CODE § 1798.105(d)(6) (West 2020).

[123] *See* § 1798.140(s)(8) (limiting the definition of research to purposes that are not commercial); § 1798.140(f) (defining "commercial purposes").

[124] Gidus, *supra* note 121.

[125] Alexis Cocco & Kimberly Gold, *CA Legislators Confront CCPA Health and Research Dangers with 'Urgency Statute' Proposal*, IAPP (Feb. 25, 2020), https://iapp.org/news/a/ca-legislators-confront-ccpa-health-and-research-dangers-with-urgency-statute-proposal [https://perma.cc/LK9N-ZXDD].

[126] Even though the CCPA contains a limited research exemption, industry stakeholders have sought clarification. *Id.*

[127] *Id.*

[128] Assemb. B. No. 713, 2019-2020 Reg. Sess. § 1798.130 (Cal. 2019) (enacted) ("The provisions of th[e proposed] act would mitigate that harm . . . by preserving access to information needed to conduct important health-related research that will benefit Californians.").

[129] *Id.* As an "urgency statute," the bill is identified as recognizing and remedying a pressing concern and would thus take effect immediately upon signature by the California governor. CAL. CONST. art. IV, § 8(d).

modern era, which is projected to see more easily contractible viruses and antibiotic-resistant bacteria.[130]

3. Data Protection Authorities: GDPR and CPRA

The implementation of the GDPR was and continues to be a massive stride towards creating a comprehensive data privacy regime in the European Union. Nonetheless, application of its research exemptions to scientific and medical research had initially been widely misunderstood, debated, and inconsistently applied across the European Union.[131] These problems ultimately led to "confusion and adverse effects" for research.[132] To remedy misapplication across the data spectrum, and in light of the sensitivity of personal data, Member States are required to delegate the supervision of data privacy regulation to data protection authorities.[133] Specifically, the GDPR mandates that each Member State has one or more independent public supervisory authority.[134] Belgium is one of the Member States that adopted such an authority.[135] The Belgian Data Protection Authority, which supervises Belgium's application of the GDPR, has been proactive in designing and implementing strategic plans, releasing annual performance reports, and imposing fines when necessary.[136]

This mandated delegation by the GDPR may be effective, considering the functional independence of agencies in the European Union.[137] It may also be true, however, that the mandate

---

[130] *See* Bill Gates, *The Next Outbreak? We're Not Ready*, TED TALK, at 0:30 (2015), https://www.ted.com/talks/bill_gates_the_next_outbreak_we_re_not_ready/transcript?language=en [https://perma.cc/W8FT-NMYD] ("Today the greatest risk of global catastrophe . . . . [is] most likely to be a highly infectious virus."). The World Health Organization has declared that Anti-microbial Resistance (AMR) is one of the top ten developing global public health threats facing humanity and requires urgent multi-sectoral action in order to achieve the Sustainable Development Goals. *Antimicrobial Resistance*, WORLD HEALTH ORG. (Oct. 13, 2020), https://www.who.int/news-room/fact-sheets/detail/antimicrobial-resistance [https://perma.cc/5AMQ-4N5J].

[131] Philipp G. H. Metnitz et al., *The General Data Protection Regulation and Its Effect on Epidemiological and Observational Research*, 8 LANCET 23 (Oct. 29, 2019), https://www.thelancet.com/journals/lanres/article/PIIS2213-2600(19)30411-4/fulltext [https://perma.cc/63ZA-MK8E] ("The application of these exemptions to clinical research has been misunderstood and debated. . . . [T]he application is inconsistent throughout the EU, leading to confusion and adverse effects for the delivery of clinical research.").

[132] *Id.*

[133] GDPR, *supra* note 27, art. 51, ¶ 1.

[134] *Id.*

[135] *Belgian Data Protection Authority Releases 2019 Annual Report*, HUNTON ANDREWS KURTH (Oct. 7, 2020), https://www.huntonprivacyblog.com/2020/10/07/belgian-data-protection-authority-releases-2019-annual-report [https://perma.cc/A2VN-RY8F].

[136] *Id.*

[137] Independence in this context "generally refers to a status which ensures that the body concerned can act completely freely, without taking any instructions or being

is limited from both a macro and micro perspective. From the macro perspective, the Member States, the data protection authorities, and the agencies and institutions operating cross-nationally may benefit greatly from an overarching parental authority that would ensure consistent interpretation and application of the GDPR. From the micro perspective, the uniquely sensitive and valuable nature of biometric data may demand the imposition of a secondary auxiliary group that focuses more directly on the flow and protection of biometric data.

States in the European Union are not alone in their adoption of data protection authorities. In November 2020, California passed the CPRA, which complements the CCPA by mandating a data protection authority, the California Privacy Protection Agency (CPPA), to establish and enforce more rigid boundaries of both of the California privacy acts' terms and provisions.[138] The CPRA refers to the CPPA as a "supervisory authority," but the CPPA mirrors the GDPR's data protection authorities in purpose and structure, as it is the body responsible for investigation and enforcement.[139] The CPPA maintains the authority to fine violators, hold hearings about alleged privacy violations, and clarify privacy guidelines.[140]

The implementation of the CPPA also moves California further from the standard American model of enforcement, by which data privacy laws are enforced by state attorneys general.[141] The CPRA gives the CPPA exclusive authority to interpret, investigate, and enforce California data privacy law.[142] It also subsidizes the CPPA's operations to fund enforcement tasks.[143] The

---

put under any pressure." Ellen Vos et al., Eur. Parliament Pol'y Dep't for Citizens' Rts. & Const. Affs., *EU Agencies and Conflicts of Interests*, PE 621.934, at 14, (Jan. 2020), https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621934/IPOL_STU(2020)621934_EN.pdf [https://perma.cc/V2EA-6VGB]. European Union agencies are expected to remain independent as far as "commercial, national or political influence." *Id.* at 13.

[138] The CPRA amends the CCPA to strengthen the "rights of California residents" by "establishing a new government agency for state-wide data privacy enforcement called the California Privacy Protection Agency (CPPA)." *California Privacy Rights Act (CPRA): CCPA vs CPRA*, COOKIEBOT (Nov. 25, 2020), https://www.cookiebot.com/en/cpra [https://perma.cc/A36R-CFT3]. *See generally* CPRA, Prop. 24, *supra* note 29 (establishing the California Privacy Protection Agency and explaining its structure and authority).

[139] CPRA, Prop. 24, *supra* note 29, at 71–72.

[140] *Id.* at 72–73.

[141] Dominic Dhil Panakal, *The CPRA Will Bring New Rights, Responsibilities and Regulators to California Data Privacy Law*, NAT'L L. REV. (Oct. 8, 2020), https://www.natlawreview.com/article/cpra-will-bring-new-rights-responsibilities-and-regulators-to-california-data [https://perma.cc/HP8E-AE45].

[142] CPRA, Prop. 24, *supra* note 29, at 71.

[143] Heather McArn & Judith Selby, *What You Need to Know About California's New Voter-Approved California Privacy Rights Act*, JD SUPRA (Dec. 17, 2020), https://www.jdsupra.com/legalnews/what-you-need-to-know-about-california-82510 [https://perma.cc/MB94-HAP6].

agency consists of five members appointed by California government officials including the Governor, Attorney General, State Senate, and Speaker of the Assembly.[144]

The California legislature's imposition of a supervisory authority that receives proper funding is an exceptional stride towards comprehensive data protection. Time will dictate whether the model outlined in the CPRA is sufficient to carry the increasing weight of personal data storage and usage by major corporations, research organizations, and other third-parties. Further, candidates' appointments for inclusion in the agency should ideally not be influenced by those appointees' respective political affiliations. Another important consideration is whether the individuals in charge of creating this authority are capable of removing their political biases to ensure protection and further scientific objectives greater than themselves.[145]

B. Disclaimer: A Federal Statute Is Not Coming Soon

To complement this note's overarching discussion of a single state regime, it is essential to provide a disclaimer: biometric data privacy may be effectively achieved by a comprehensive federal data privacy statute.[146] A federal biometrics privacy statute may provide the highest level of protection for the greatest number of people compared to a state-centric, sectoral regime[147] through which some states may endorse insufficient privacy statutes and others may not endorse any at all.[148] Further, differing state regimes make it more difficult for businesses to function inter-state.[149] Thus, from an economic standpoint, varying state regimes may stifle business, particularly for new and smaller businesses lacking the resources to conform their practices to many different guidelines

---

[144] Panakal, *supra* note 141.

[145] *See generally* Colin J. Bennett & Smith Oduro-Marfo, Privacy, *Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities*, U. OF VICTORIA (Oct. 2019) (recognizing the power of data protection authorities to collect data and the influence that data has on elections and the political process).

[146] *See, e.g.*, Zimmerman, *supra* note 8, at 637 (arguing that a federal law governing biometric data privacy is necessary because biometric characteristics are increasing in popularity as a form of identification, are permanent, and cannot be changed like other forms of identification).

[147] *Id.* at 668.

[148] *See id.* A federal regime is also being called upon to harmonize the US regulatory framework with the framework of other regulations like the GDPR. *See* Crescioni & Sklar, *supra* note 19, at 126–27.

[149] Zimmerman, *supra* note 8, at 650–51 ("As more states implement biometric information privacy statutes in the future, the difficulty [for businesses] of abiding by each individual definition will increase.").

and thus to successfully expand.[150] Finally, a federal statute, unlike state statutes, would provide one uniform definition of "research," as opposed to conflicting definitions under multiple state regimes, and can prescribe one overarching data protection authority.

Yet, in the United States, a number of federal statutes enacted prior to the rise of biometric data were conclusively, albeit understandably, unprepared to protect such data.[151] Currently, there are few, if any, true limits on biometric data collection, and private companies are free to collect and use biometric data for whatever purposes they see fit.[152] Many companies have taken advantage of public ignorance by employing privacy statements that demand full data-analytical control over personal data in exchange for services and burying such statements in service contracts,[153] despite the fact that people neglect to read these statements.[154]

While there are existing federal statutes that attempt to regulate personal information collected via electronic communications, none of these statutes include specific provisions for the processing, retention, or protection of biometric data.[155] For example, the Genetic Information Nondiscrimination Act of 2008 (GINA) is one federal statute that focuses on biometric information, but only for the purposes of "protect[ing] individuals from discrimination based on their genetic information."[156]

HIPAA contains the only federal regulation that mandates national standards of using, storing, and safeguarding biometric information collected by private entities,[157] including electronic

---

[150] *Id.* At the current rate, a business will be forced to expend their resources to make sense of and overcome the fifty-plus hurdles of conflicting state legislation.

[151] *See id.* at 644–45 (noting the lack of a federal statute regulating data processing and storage by websites, data brokers, or businesses).

[152] *See id.* at 639. This perpetuates behavior by private companies to weaponize data for self-serving purposes, without consumers being privy to who or what has the data and what is being done with it. *See* PASQAULE, *supra* note 6, at 10.

[153] Alan McQuinn, *The Economics of "Opt-Out" Versus "Opt-In" Privacy Rules*, INFO. TECH. & INNOVATION FOUND. (Oct. 6, 2017), https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules [https://perma.cc/YE25-SHPU].

[154] Beyond users' rare consultation of a website's privacy policy, users often have "inaccurate perceptions about their own knowledge of how online technologies may affect their privacy." *Id.*

[155] Two federal statutes that attempt to regulate personal information collected via electronic communications are the Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501–6506, which regulates websites' collection and use of children's personal information by requiring parental consent, and the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2523, 2701–2711, which regulates the interception of general communications. Neither includes specific provisions for the processing, retention, *and* protection of biometric data. *See* Zimmerman, *supra* note 8, at 645.

[156] *Id.* at 646; Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of Titles 26, 29, and 42 of the United States Code).

[157] Zimmerman, *supra* note 8, at 645.

health care transactions and unique health identifiers.[158] HIPAA's intended purpose is virtuous: "to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's . . . well being."[159] But HIPAA falls short in both its language and application. HIPAA restrictions apply *only* to "covered entities," including health care providers, health plan sponsors, health care clearinghouses, and their business associates or subcontractors.[160] It does not otherwise apply to entities that are not healthcare providers.[161] The Health Information Technology for Economic and Clinical Health (HITECH) Act[162] attempted to fill these gaps, but only does so in a very narrow set of circumstances.[163] This means that Apple and Amazon (and many future collectors of your biometric data) are not subject to these restrictions, and may thus share your information with third-parties without your consent.[164]

The Federal Trade Commission (FTC) Act,[165] enforced by the FTC, attempts to fill the gaps caused by the narrow scope of HIPAA by imposing additional requirements on any entity that creates, receives, maintains, or transmits personal health information.[166] Moreover, data privacy experts consider the FTC to be the "'de facto' federal data protection authority."[167] But the

---

[158] For example, a covered entity must remove biometric identifiers, including finger and voice prints, for health information to be rendered as "not 'individually identifiable health information," and thus not subject to certain provisions. *Id.* (quoting 45 C.F.R. § 164.514(b)(2)(i)(P)).

[159] U.S. DEP'T OF HEALTH & HUM. SERVS., OCR BRIEF: SUMMARY OF THE HIPAA PRIVACY RULE 1 (May 2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/X8PQ-T4YJ].

[160] *See* 45 C.F.R. § 160.103 (defining "business associate" and "covered entity"); *Covered Entities and Business Associates*, HHS.GOV (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html [https://perma.cc/9S6N-JQCR].

[161] *Id.*

[162] The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 and "addresses the privacy and security concerns associated with the electronic transmission of health information." *HITECH Act Enforcement Interim Final Rule*, HHS.GOV (June 16, 2017), http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html [https://perma.cc/B6YD-HHNV].

[163] The HITECH Act established a data breach notification requirement for brokers that were not "covered entities" under HIPAA but that process personal health records. *See* PETER SWIRE & DEBRAE KENNEDY-MAYO, *supra* note 83 at 21.

[164] *See The Access Right, Health Apps, & APIs*, HHS.GOV (Jan. 6, 2021), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html [https://perma.cc/8FVE-T8NN]. For an explanation of the limitations of covered entities under HIPAA, see *supra* Section I.B.

[165] 15 U.S.C. §§ 41–58.

[166] *See Sharing Consumer Health Information? Look to HIPAA and the FTC Act*, HHS.GOV (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/sharing-consumer-health-information-look-hipaa-ftc-act [https://perma.cc/SJ8C-3993].

[167] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014).

primary purpose of the FTC Act is not to regulate biometric data from improper use,[168] and the FTC is not suited to fully protect biometric data, nor to fully understand the intricacies of data collection, processing, and privacy.[169]

Thus, while federal regulation of sensitive personal data would likely provide the most comprehensive protection to consumers, such an endeavor is unlikely to be successfully developed and implemented in the near future. Accordingly, state legislatures must take it upon themselves to craft laws that will adequately protect their constituents.

III. NEW YORK STATE AND THE NEW YORK PRIVACY ACTS

New York State's endeavor to create its own comprehensive data privacy statute has been an uphill battle.[170] Both of the NY Privacy Acts faced criticism as the most expansive privacy acts in the United States to date;[171] the acts' respective novelties may make that proverbial hill more difficult to climb.

A. History of Data Privacy Protection in New York (and Its Lack Thereof)

New York first implemented data breach notification laws in 2005.[172] The New York State Information Security Breach and Notification Act[173] requires state entities and businesses that own or license data consisting of private information of New York residents[174] to inform residents and

---

[168] The purpose of the FTC Act is to prevent "unfair methods of competition" and "unfair or deceptive acts or practices" in business or commerce generally. *See* 15 U.S.C. § 45(a)(2).

[169] *See* Solove & Hartzog, *supra* note 167, at 600 (noting that critics refer to the FTC as "weak and ineffective" in the data protection role).

[170] Beyond any expected delays posed by COVID-19 in 2020, NYPA has been continuously rejected and tabled for the last three years. *See* Trebicka et al., *supra* note 49 (noting that in May 2019, NYPA was forwarded to the Consumer Protection Committee of the New York State Senate, which held a Joint Public Hearing on the Act, and on November 22, 2019, the Senate held a public hearing on general privacy legislation.).

[171] The NYPA is novel in its implementation of an opt-in regime for the processing of data, such that consumers would need to explicitly consent to have their data collected. S.B. 6701, 2021-2022 Reg. Sess. (N.Y. 2021)/Assemb. B. 680A, 2021-2022 Reg. Sess. (N.Y. 2021); Trebicka et al., *supra* note 49. The BPA similarly requires "a written release executed by the subject of the biometric identifier." Assemb. B. 27, 2021-2022 Reg. Sess. (N.Y. 2021).

[172] *See* Trebicka et al., *supra* note 49.

[173] N.Y. GEN. BUS. LAW § 899-aa (McKinney 2019); N.Y. STATE TECH. LAW § 208 (McKinney 2019).

[174] "Private information" under the state Information Security Breach and Notification Act includes "personal information consisting of any information in combination with [biometric information], when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired." *Id.* § 899-aa(1)(b).

credit reporting agencies if a breach occurred that compromised a resident's personal information.[175]

On March 21, 2020, New York's Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) went into effect.[176] The purpose of the SHIELD Act is to broaden the scope of the data breach notification law.[177] The SHIELD Act requires "[a]ny person or business that owns or licenses computerized data which includes private information of a resident of New York [to] develop, implement and maintain reasonable safeguards to protect . . . private information."[178] However, the SHIELD Act, similar to other data privacy acts in New York and elsewhere, fails to mandate any specific safeguards or compliance procedures that would provide sufficient protection for consumers.[179]

Despite the gaps in existing legislation, New York has yet to enact a functioning and comprehensive biometrics privacy act, but instead has amended existing acts to regulate biometric data.[180] To the detriment and chagrin of all who prefer blanketed protection, the current approach leaves gaps in protection and uncertainty regarding the scope of the law.[181]

B. How Do the New York Privacy Acts Square Up?

The NY Privacy Acts have progressive restrictions but fail to sufficiently protect the preservation of data for research.

---

[175] "Personal information" under the state Information Security Breach and Notification Act means "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." *Id.* § 899-aa(1)(a).

[176] *Id.* § 899-bb.

[177] Trebicka et al., *supra* note 49.

[178] *Id.* § 899-bb(2)(a).

[179] The SHIELD Act states that compliance requires an organization to institute a data security framework that considers "reasonable administrative, technical and physical safeguards," but the factors constituting a single violation are unclear. *Id.* § 899-bb(2)(c); *see* Brian G. Cesaratto, *The New York State "Stop Hacks and Improve Electronic Data Security Act" (SHIELD Act) Becomes Effective March 21, 2020: Is Your Organization Ready to Achieve Compliance?*, NAT'L L. REV. (Feb. 6, 2020), https://www.natlawreview.com/article/new-york-state-stop-hacks-and-improve-electronic-data-security-act-shield-act#:~:text=The%20law%20broadly%20requires%20that,integrity%20of%20the%20private%20information.%E2%80%9D [https://perma.cc/DE5X-9E3R].

[180] For example, the proposed BPA would be enacted as part of New York's General Business Law. *See* New York Biometric Privacy Act, Assemb. B. 27, 2021-2022 Reg. Sess. (N.Y. 2021). As currently written, the bill is sparse compared to the more comprehensive protections provided by the combined CCPA and CPRA.

[181] *See, e.g.*, Stephen E. Breidenbach & Terese L. Arenth, *Navigating the Ambiguous Requirement of 'Reasonable Security' Measures While Protecting Personal Information*, LAW.COM (May 8, 2020, 2:10 PM), https://www.law.com/newyorklawjournal/2020/05/08/navigating-the-ambiguous-requirement-of-reasonable-security-measures-while-protecting-personal-information [https://perma.cc/V38X-XW5Z] (explaining that different acts will impose separate but overlapping security requirements depending on a variety of factors).

The NYPA includes a right to erasure, similar to the GDPR and the CCPA.[182] The BPA alone does not include any right to erasure after initial consent by the subject or consumer,[183] but biometric information under the BPA would likely be subject to erasure under the relevant provisions of the NYPA.[184]

Under the NYPA, a controller, the person or entity who determines the purposes and means of the personal data processing,[185] is not required to comply with a consumer's request to delete personal data if that controller needs to maintain such data for "public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws."[186] Further, the controller's deletion of such data must be likely to seriously impair, or make impossible, the research efforts and its ultimate purpose.[187] Finally, the consumer must have provided informed consent and the personal data must not have been processed for any purpose other than such research.[188]

However, neither of the NY Privacy Acts include a clear definition of research, nor a clearly defined scope for their research exemptions. This means that permissible uses of data for research may be subject to inconsistent interpretation by courts, agencies, and research participants in ways that may be over- or underinclusive. Further, unlike the GDPR and the CPRA, neither of the NY Privacy Acts prescribe any data protection authority. As demonstrated by the CCPA's own endeavors, such an authority is vital to maintain the integrity of data protection.[189]

Moreover, the NY Privacy Acts adopt an "opt-in" regime, meaning New Yorkers would have to explicitly consent to have businesses collect and store their data.[190] The GDPR, but not the

---

[182] S.B. 6701, 2021-2022 Reg. Sess. (N.Y. 2021)/Assemb. B. 680A, 2021-2022 Reg. Sess. (N.Y. 2021).

[183] *See* Assemb. B. 27.

[184] The NYPA's definition of "personal data" includes nonspecific and nonlimiting language that would seemingly include "biometric information." S.B. 6701/Assemb. B. 680A.

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] *See supra* Section II.A.2 (demonstrating that research suffered due to uncertainties in scope and application); *see also* GDPR, *supra* note 27, at art. 51, ¶ 1 (explaining that DPAs exist to "protect the fundamental rights and freedoms of natural persons . . . and to facilitate the free flow of personal data"); *The U.S. Urgently Needs a Data Protection Authority*, ELEC. PRIV. INFO. CTR., https://epic.org/dpa [https://perma.cc/CZ26-W97X] (explaining that an independent data protection agency is needed in the United States because data breaches have reached epidemic-level proportions).

[190] Trebicka et al., *supra* note 49, at 3 ("The 'opt in' [regime] requires the consumer to make—and the company to record—'a clear affirmative act establishing a

CCPA, chose to invoke this type of scheme.[191] This opt-in framework flips conventional American privacy law on its head, while necessarily maintaining consent as the "sine qua non" of data retention.[192] Despite opt-in regimes generally being a step forward for data privacy, they carry disadvantages if unrestrained in the NY Privacy Acts. This is because New York State residents, including those residing within New York City,[193] who are members of groups that are less likely to opt-in to research opportunities may also be members of groups that would be most likely to be benefit from research.[194] This is especially true if these individuals are not explicitly aware of the societal benefits of opting-in.[195]

Moreover, individuals in the United States are increasingly unwilling to sacrifice their personal data for any purpose.[196] With the introduction of an opt-in regime, and without greater incentives to participate in research, there would be even

---

freely given, specific, informed, and unambiguous indication of the agreement to the processing of personal data relating to the consumer.'" (quoting NYPA)).

[191] *See Consent—General Data Protection Regulation (GDPR)*, GDPR, https://gdpr-info.eu/issues/consent/ [https://perma.cc/UJK8-XHT8] (explaining that "[c]onsent cannot be implied and must always be given through an opt-in, a declaration or an active motion"); CAL. CIV. CODE § 1798.120 (West 2020) (establishing the right of consumers to opt-out of businesses' sale of their information).

[192] Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 598, 622 (2009) ("[US] law relies on an implied consent regime, assuming that users should simply diminish their privacy expectations for personal data once it has been tendered to commercial third parties.").

[193] *Population—New York City Population*, NYC PLANNING (Oct. 21, 2021, 11:03 AM), https://www1.nyc.gov/site/planning/planning-level/nyc-population/population-facts.page#:~:text=With%20a%20July%202015%20population,resides%20in%20New%20York%20City [https://perma.cc/5YZ3-EVXL] ("New York is the most populous city in the United States, more than twice the size of the second largest city, Los Angeles."). In the wake of an opt-in framework in such a populous city, the loss for potential data sets, and their corresponding values for research, would likely be extreme. *See* Michele Brugioni, *Findings Reveal Lack of Participants in Critical Research Is Caused by Fear*, BIOSPACE (Oct. 21, 2021, 11:03 AM), https://www.biospace.com/article/findings-reveal-lack-of-participants-in-critical-research-is-caused-by-fear-/#:~:text=A%20new%20review%20shows%20fear,were%20common%20denominators%20among%20patients.

[194] Cornelia Junghans & Melvyn Jones, *Consent Bias in Research: How to Avoid It*, 93 HEART 1024, 1024–25 (2007) ("[C]onsent requirements for recruiting patients to medical research could result in a failure to include participants who were most likely to benefit from interventions, such as older or socioeconomically deprived patients."). Notably, supervisory authorities can provide the clarity necessary to reduce this consent bias. *Id.*

[195] McQuinn, *supra* note 153 (noting that, in the case of privacy, Coase's Theorem suggests that "control over data will go to the party that values it the most," regardless of whether the individual must opt in or opt out. "This means that if the law requires individuals to opt in before a company can collect or use data, then a company may provide incentives to users to opt in to sharing their data." That company can similarly remedy the information asymmetry that naturally exists in data markets.).

[196] *See id.*; *see also* Marty Swant, *People Are Becoming More Reluctant to Share Personal Data, Survey Reveals*, FORBES (Aug. 15, 2019, 1:33 PM), https://www.forbes.com/sites/martyswant/2019/08/15/people-are-becoming-more-reluctant-to-share-personal-data-survey-reveals/?sh=3aabfe891ed1 [perma.cc/H2D7-GV26] (suggesting that individuals in the United States are becoming increasingly less likely to share personal data).

less data available for scientific researchers and clinical trials.[197] In consideration of the increased use of smart devices like wearables and self-monitoring applications that exponentially increase the pool of potential data sets, there should be *more* data for scientific, technological, and medical researchers to use, not less.

The NY Privacy Acts, compared to the GDPR,[198] are even less clear about what research is afforded an exemption. In their current forms, the NY Privacy Acts hardly recognize the need to protect usage of collected biometric data for research or for promoting public health.[199] The problem with the BPA is not simply that it fails to mandate any protections for research; it does not even mention the word "research."[200] The NYPA does, at least, mention the word "research" in the context of its research exemption, which exempts from deletion personal data collected for the following purpose:

> [T]o engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, provided that the consumer has given informed consent and the personal data is not processed for any purpose other than such research.[201]

To be clear, the NY Privacy Acts impose revolutionary data privacy restrictions relative to those of other states, especially as they act in conjunction with one another given their broad definitions of personal data or biometric information, opt-in requirements, explicit private rights of action, and the NYPA's imposition of a "data-fiduciary" obligation on relevant entities.[202]

---

[197] *See* McQuinn, *supra* note 153 ("[O]pt-in requirements frame consumer choices in ways that lead to less-than-optimal data sharing.").

[198] See *supra* Section II.A.2 for a discussion of the research exemption under the GDPR.

[199] Currently, the NYPA has a short section on protections for research, under which it is necessary "to engage in public or peer-reviewed scientific, historical, or statistical research in the public interest . . . when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research." S.B. 6701, 2021-2022 Reg. Sess. (N.Y. 2021)/Assemb. B. 680A, 2021-2022 Reg. Sess. (N.Y. 2021). The BPA alone does not set forth any protections for research nor does it even mention the word "research." *See* Assemb. B. 27, 2021-2022 Reg. Sess. (N.Y. 2021).

[200] *See* Assemb. B. 27.

[201] S.B. 6701/Assemb. B. 680A.

[202] Alexander H. Southwell & Mylan L. Denerstein, *New York Privacy Act Update: Bill Out of Committee, Moves to Full Senate*, GIBSON DUNN (May 21, 2021), https://www.gibsondunn.com/new-york-privacy-act-update-bill-out-of-committee-moves-to-full-senate [https://perma.cc/6QZ2-LVZ3]. Professor Jack M. Balkin is credited with introducing the data or information fiduciary concept, later adopted in NYPA. David E. Pozen & Lina M. Khan, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 497 (2019). As per this concept, "online service providers and cloud companies who collect, analyze, use, sell, and distribute personal information should [have an elevated duty] . . . toward their customers and end-users" (similar to the fiduciary duty concept). Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186, 1209 (2016).

As a result, consumers residing in New York will be much more protected compared to consumers in other states, but scientific research and participation in clinical trials will likely suffer, as they did in the European Union and in California.[203] Uncertainty in application of the law is chaos; it leads to an overwhelming increase in litigation.[204] Finally, the NY Privacy Acts may be less likely to pass with looming uncertainties following the burdens imposed by their current restrictions, such as the concerns expressed over the NYPA's creation of a private right of action during the Committee on Consumer Protection and the Committee on Internet and Technology's Joint Public Hearing.[205]

IV. SOLUTION: A TRIPARTITE DEFINITION AND THE GATEKEEPERS OF RESEARCH

The NY Privacy Acts will better reflect the balance between the need for scientific development and individual privacy and autonomy if lawmakers more clearly define the research exemption to the erasure of biometric data and mandate the imposition of data protection authorities. Section IV.A establishes that the NY Privacy Acts should update their definitions of research and the scope of the research exemptions therein. Section IV.B proposes a data protection authority and a biometric subcommittee that would evaluate the processing of personal data and biometric information for research, as directed by the updated NY Privacy Acts' provisions.

A. A Tripartite Definition and Scope of the Research Exemption

Research under the NY Privacy Acts deserves to be clearly defined, and the scope for its exemptions, sufficiently described.

---

[203] *See supra* Section II.A.2; *see also* Effy Vayena et al., Eur. Parliament Panel for the Future of Science and Technology, *How the General Data Protection Regulation Changes the Rules for Scientific Research*, PE 634.447, at 9 (July 2019), https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf [https://perma.cc/8C66-HBQ7] ("Expected risks include the possibility that the GDPR might place an excessive burden on researchers and research participants, increase the time needed to obtain IRB/ERC approval with consequent delays in project development, undermine attempts to develop a dynamic consent system, and potentially result in negative consequences for epidemiologic research caused by the GDPR's requirement to treat pseudonymised data as personal data.").

[204] Professors William Landes and Richard Posner theorize that greater uncertainty leads to a greater likelihood of litigation. William Landes & Richard Posner, *Legal Precedent: A Theoretical and Empirical Analysis*, 19 J.L. & ECON. 249, 249–50 (1976). This holds true for New York's private right of action, which mimics the Illinois Supreme Court's broad interpretation of the private right of action under the Illinois Biometric Information Privacy Act in their ruling of *Rosenbach*. *Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197 (Ill. 2019).

[205] Trebicka et al., *supra* note 49, at 8.

In crafting such a definition and scope, New York legislators should borrow concepts from the GDPR, the CCPA and CPRA, and "open science," which recognizes the value of secondary processing to scientific, technological, and medical research.

1. Research—Hanging in the Balance

Transparency and informed consent are at the crux of both data privacy and research.[206] Without a clear research exemption and an adequately knowledgeable data protection authority, researchers and research institutions may not know whether the data sets used by their respective research projects are exempt, or whether they are taking proper steps toward protecting biometric data—which is a different beast that deserves elevated protection compared to other types of personal data.[207]

If the research exemption is too narrow, it may limit progress in science, medicine, and technology.[208] Biometric data is increasingly important for research such as longitudinal epidemiological and genetic studies, as well as collaborative studies where accurate identification of subjects over time can be difficult.[209] This holds especially true in an era that is projected to see a sharp increase in disease, easily-contractable viruses, and antibiotic resistant bacteria.[210] Thus, a properly defined research exemption can help promote health among the New York populace.

At the other extreme, if the definition of research is overly broad, it may permit for-profit companies to use and sell consumer

---

[206] *See* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles: Implementation and Mapping of Fair Information Practices*, at 6–7 (Nov. 2006), https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf [https://perma.cc/YL7B-S64U] (noting that the seven Global Privacy Standard privacy principles include consent and transparency).

[207] See *supra* Section I.A for an explanation of the dangers of biometric data collection, processing, and storage.

[208] *A Preliminary Opinion on Data Protection and Scientific Research*, EUR. DATA PROT. SUPERVISOR 21 (Jan. 6, 2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf [https://perma.cc/FH9E-RFRV] (explaining that a substantial number of people rejecting or being excluded from, scientific research "may have a negative effect on the representativeness and reliability of the research data and thus on the integrity of research").

[209] Patricia M. Corby et al., *Using Biometrics for Participant Identification in a Research Study: A Case Report*, 13 J. AM. MED. INFORMATICS ASS'N. 233, 233 (2006) ("[I]dentification of subjects over time can be difficult when the subject may be young or an unreliable source of identification information.").

[210] Gates, *supra* note 130, at 0:30 ("Today the greatest risk of global catastrophe . . . [is] most likely to be a highly infectious virus."); *Antimicrobial Resistance*, *supra* note 130 (stating that "WHO has declared [antimicrobial resistance as] one of the top [ten developing] global public health threats facing humanity" and that "[antimicrobial resistance] requires urgent multisectoral action in order to achieve the Sustainable Development Goals").

data to expand their own research and development efforts under the guise of the "public interest" or "public health."[211] Imagine that a technology company is capable of collecting biometric data that, in conjunction with other data markers, is fed into a complex algorithm, only to paint a flawed picture of an individual and his or her health status. Because these technology companies are not health providers collecting health data,[212] that data may be packaged with other data sets and sold to insurance companies,[213] which use and rely on that information to increase that individual's insurance premiums.[214] Thus, the exemption should not apply to uses of the data if the primary or secondary purposes for the uses are commercial benefit.

Ultimately, the goal in drafting the language for the research exemption must be to find balance—to promote innovation without permitting exploitation of people's biometric data. This goal can be achieved, in part, by leveraging the theoretical proposition of "open science," which recognizes extraordinarily valuable and currently unrealized benefits to the public welfare in reasonably accessible research and data.[215]

2. Breaking Down the Proposed Research Exemption and Scope

The New York legislature should amend the NY Privacy Acts to adopt a unified definition of "research" that is effectively a combination of the respective definitions of research in the

---

[211] In the similar context of HIPAA research exemptions, "[p]ublic health authorities or third party researchers could simply obtain the desired [personal health information] under the guise of the public health exception to avoid . . . review." Andrea Wilson, *Missing the Mark: The Public Health Exception to the HIPAA Privacy Rule and Its Impact on Surveillance Activity*, 9 HOUS. J. HEALTH L. & POL'Y 131, 151 (2008).

[212] For example, Apple's Health Record API may not be subject to HIPAA regulations because Apple does not store patient data on its servers. *The Access Right, Health Apps, & APIs*, *supra* note 164; see also *supra* Section I.B for an explanation of the limitations on covered entities and data under HIPAA.

[213] The NYPA recognizes activities similar to the one described here as "automated decision-making," which is defined as "a computational process, including one derived from machine learning, artificial intelligence, or any other automated process, involving personal data that results in a decision affecting a consumer," and provides for an appeal process for such decisions. S.B. 6701, 2021-2022 Reg. Sess. (N.Y. 2021)/Assemb. B. 680A, 2021-2022 Reg. Sess. (N.Y. 2021).

[214] This is a real and pressing issue according to Professor Frank Pasquale. Telephone Interview with Frank Pasquale, Professor of Law, Brooklyn Law School (Oct. 16, 2020) (notes on file with author); PASQUALE, *supra* note 6, at 27–28 ("[T]he ACA . . . includes provisions promoting insurance discounts in exchange for participation in 'wellness programs.' Verifying that participation (in activities ranging from meditation to running) can only expand the market for bodily surveillance and quantified selves.").

[215] *See generally* Bobbie A. Spellman et al., *Open Science: What, Why, and How*, PSYARXIV (Apr. 18, 2017) (manuscript), https://doi.org/10.31234/osf.io/ak6jr [https://perma.cc/6RDM-YM92] (primer on open science movement).

CCPA and GDPR, with a reasonable degree of added reverence for the "open science" concept.

First, the legislature should amend the NY Privacy Acts to adopt the CCPA's definition of "research" as "scientific, systematic study and observation, including basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health."[216] The NY Privacy Acts should incorporate the same baseline requirements as the CCPA for the processing of personal data for research, reflecting the seven principles of lawful data processing,[217] and including the practical employment of technical safeguards and complete deidentification.[218] This definition and its corresponding elaboration on exemption explains the defined boundaries of research in terms of both process and purpose, while considering industry-specific ethical standards and long-standing regulations.

To narrow the scope of the definition, the NY Privacy Acts should borrow from the GDPR an evolving list of specific applications, like "technological development and demonstration, fundamental research, applied research and privately funded research . . . studies conducted in the public interest in the area of public health."[219] The NY Privacy Acts should similarly reject scientific research projects that fail to abide by relevant industry-specific ethical standards, or that are otherwise not in conformity with good practice.[220] A data protection authority could then actively adjust the confines of good practice and clarify relevant industry-specific standards as they are confronted or anticipated.

In the interest of limiting privacy infringements, the legislature should completely reject exemptions for research where the primary or secondary purposes of processing such biometric data would be commercial benefit.[221] The data protection authority proposed in Section IV.B should be responsible for rendering the final decision as to whether a commercial benefit is a primary or secondary purpose of an entity's data collection; admittedly this would not be an easy or

---

[216] CAL. CIV. CODE § 1798.140(s) (West 2020).

[217] Cavoukian, *supra* note 206.

[218] Among the other clarifications provided by the CCPA's definition of research is a requirement for entities to employ business processes to prevent inadvertent disclosure, and to limit physical access to the data. § 1798.140(s).

[219] GDPR, *supra* note 27, at recital 159.

[220] Ducato, *supra* note 102.

[221] The CCPA defines commercial purpose as a means "to advance a person's commercial or economic interests, such as by inducing another person to buy, rent, lease, join, subscribe to, provide, or exchange products, goods, property, information, or services, or enabling or effecting, directly or indirectly, a commercial transaction." CAL. CIV. CODE § 1798.140 (West 2020).

straightforward determination, but a sufficiently resourced authority would be best-suited to engage in this analysis. Assuming that neither the primary nor secondary purposes of data retention are commercial benefit, businesses should continue to provide notice to the initial provider of such data through methods that would not sacrifice the identity of the initial provider. Regulated entities should also have an ongoing obligation to adopt modern, highly effective methods of deidentification, like FHE.[222] Further, the NY Privacy Acts should provide exemptions for certain businesses engaging in research for the public welfare, like Apple and its research application, only if those businesses do not reidentify or attempt to reidentify any deidentified biometric information.

Inspired by the open science concept, the NY Privacy Acts should explicitly permit secondary processing of data for research purposes. Secondary processing would similarly be conditioned on neither the primary nor the secondary purposes of such use being for commercial benefit. Under the proposed structure, the New York data protection agency would need to check a business's purported qualified purposes for any and all secondary uses.

Justifying this proposed definition of the research exemption involves balancing three considerations. First, personal data is not mutually exclusive; data is an intangible, nonrivalrous good.[223] In other words, assuming that the data is completely deidentifiable, a researcher's use will not preclude the data owner's use.[224] Second, a properly balanced exemption would immensely benefit society. As discussed in Part I, secondary use of biometric data has the potential to greatly expand our understanding of human health and behavior and to improve the quality of care for patients and others suffering from various illnesses.[225] Third, the exemption process would be

---

[222] See *supra* Section I.B for a presentation of current standards and new alternatives for deidentification. *See* Gil, *supra* note 80.

[223] Charles I. Jones & Christopher Tonetti, *Nonrivalry and the Economics of Data* (STANFORD GRADUATE SCH. OF BUS., Working Paper No. 3716, 2019), https://www.gsb.stanford.edu/faculty-research/working-papers/nonrivalry-economics-data [https://perma.cc/E9AN-DTVF] (recognizing that, because data is infinitely usable, there are major potential societal gains to designations whereby the same data is used by multiple firms simultaneously).

[224] MIT Tech. Rev. Insights, *Data's Identity in Today's Economy*, MIT TECH. REV. (Apr. 7, 2016), https://bit.ly/3sn2J9Q [https://perma.cc/EWV9-46CE] (quoting Oracle's big-data strategist: "[a] single piece of data can fuel multiple algorithms, analytics, and applications simultaneously [without depletion]"). Nonetheless, the legal norm applied to data across the spectrum is that it is property that can be owned. *See id.*

[225] S.M. Meystre et al., *Clinical Data Reuse or Secondary Use: Current Status and Potential Future Progress*, 2017 IMIA YEARBOOK OF MED. INFORMATICS 38, 38, (explaining that an environment that recognizes secondary use could see a significant

premised on sufficient security measures being in place to prevent misuse by third-parties, provided by requirements like deidentifiability,[226] plus the added perpetual layer of security provided by an in-state data protection authority.[227]

B. The Gatekeepers of Research: Guardians of Biometric Data in the Empire State

A New York data protection authority and a biometric data subcommittee should assume responsibilities similar to those of the GDPR and CPPA. Beyond interpreting and enforcing the provisions of the NY Privacy Acts and protecting consumers from malicious uses of their personal data and processing methods that are insufficiently secure, these "gatekeepers" should be imbued with the power to qualify research data for secondary processing.

1. Proposal for the Adoption of the New York Data Protection Authority

New York should adopt a New York data protection authority (Data Authority) that will, like those mandated by the GDPR and CPRA,[228] have the power to provide expert advice on data protection issues and handle complaints arising from violations of the NY Privacy Acts. Similar to the CPPA, the Data Authority may consist of appointees by the governor, attorney general, state senate, and speaker of the assembly. Nonetheless, the Data Authority should be prepared to expand its unit of data privacy experts as time progresses; this will increase its capacity to handle the inevitable rise in demand and collection of personal data and NY Privacy Acts violations and complaints arising therefrom.[229]

First, the Data Authority could approve, reject, or require modifications to a given data sharing plan, or the process by which it shares deidentified data with other entities. A nonprofit business

---

reduction in the "administrative and data capture burden on clinicians;" a dramatic reduction in "the time for clinical data to be available for public health emergencies and for traditional public health purposes;" and a "profound[reduction in] the cost for communicating, duplicating, and processing healthcare information").

[226] *See supra* Part I. There are current and future methods in place for the effective deidentification or anonymization of personal data. For added protection, the integrity of these methods should ideally be checked by a data protection authority.

[227] *See infra* Section IV.B.

[228] *See* GDPR, *supra* note 27, art. 51 (requiring each Member State to create a public supervisory authority for ensuring enforcement of the GDPR); *see also* CAL. CIV. CODE § 1798.199 (West 2020) (establishing the CPPA and explaining its structure and authority).

[229] Venky Anant et al., *The Consumer-data Opportunity and the Privacy Imperative*, MCKINSEY & CO. (Apr. 27, 2020), https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative [https://perma.cc/W2EB-V2S7].

or research organization may be required to submit an application to use biometric data for research purposes, a detailed protocol outlining the methods of processing and deidentification, and mandatory informed consent forms clearly identifying data subjects' consent in order to be eligible for review.

Second, assuming the role of an ethics board, the Data Authority may orchestrate tutorials on ethical open science to educate researchers and related institutions on their responsibilities as data fiduciaries. Assuming the role of a regulatory body, the Data Authority would be responsible for ensuring that all applicants approved to engage in biometric data processing for research are abiding by the NY Privacy Acts' mandates. The Data Authority would also exist to ensure that researchers have received requisite consent under the NY Privacy Acts.

Under this structure, the Data Authority, as a body appointed by state government officials, would be best positioned to understand the intersection and potential conflict between data privacy regulations on the federal, state, and industry-specific and ethical standard levels. This body would be primarily responsible for interpreting provisions of the NY Privacy Acts. This structure would prevent gaps arising from conflicts with long-standing industry practices from undermining the NY Privacy Acts.[230] The Data Authority may also consistently analyze and report on the efficiency and sufficiency of deidentification methods and data sharing plans.

Ultimately, the proposed Data Authority would provide clarity and uniformity to the NY Privacy Acts' novel provisions, thereby preventing the confusion and misapplication that occurred in the European Union, California, and Illinois from the implementation of the GDPR, CCPA, and BIPA, respectively. By mandating the creation of a data protection authority, the NY Privacy Acts would actively learn from and overcome the mistakes made by their predecessors.

As discussed in Part I, BIPA's private right of action was broadly interpreted by the Illinois Supreme Court, resulting in a sharp increase in litigation.[231] The NY Privacy Acts, as drafted, similarly permit a private right of action, and would thus benefit from a narrow and uniform interpretation of the respective obligations under each act—possibly one that consciously evolves and responds to unexpected consequences, like corresponding increases in litigation. Moreover, the Data Authority would enforce

---

[230] *See supra* Part II.

[231] de la Torre et al., *supra* note 41.

the NY Privacy Acts by identifying violations and providing preliminary opinions as to whether claims are meritorious.[232]

The Data Authority would interpret any language with respect to security obligations imposed by the NY Privacy Acts, further preventing misapplication. Learning from BIPA's errors, the Data Authority can determine, on a case-by-case basis, which security measures are "reasonable."[233] This eliminates ambiguity from the "reasonable[ness]" requirement and provides approved researchers with notice of sufficient protocols.

A properly structured and sufficiently resourced Data Authority would allow New Yorkers and those affiliated with research institutions and applicable businesses in New York to enjoy the benefits of superiorly resourced scientific and medical research.[234]

2. Proposal for the Adoption of the New York Biometric Data Protection Authority

Further, the NY Privacy Acts should mandate the creation of a biometric data protection subcommittee that is better poised—in knowledge, time, and resources, as compared to a singular data protection authority that focuses on all types of data—to understand and apply the higher standards of privacy practices required by businesses and industries that use biometric data for any purpose, including research. This subcommittee, unlike its parent committee, should consist specifically of qualified experts in science, medicine, and biometric data privacy.

An in-state ethics and compliance biometric subcommittee will serve two primary functions that complement the functions of

---

[232] Preliminary opinions are also provided by other regulatory authorities, like the US Securities and Exchange Commission (SEC) and the FTC. For example, "[a]n individual or entity who is not certain whether a particular . . . action would constitute a violation of the federal securities law may request a 'no-action' letter from the SEC staff." *No Action Letters*, SEC, https://www.investor.gov/introduction-investing/investing-basics/glossary/no-action-letters [https://perma.cc/WPS8-E4PA]. If granted, the letter signifies that "SEC staff would not recommend that the Commission take enforcement action." *Id.*

[233] The data fiduciary obligation that would be imposed by the NYPA is illustrative. NYPA states that legal entities that process personal data have an obligation to "reasonably" secure personal data from unauthorized access, and to not use personal data in any way that will result in "reasonably" foreseeable harm. S.B. 6701, 2021-2022 Reg. Sess. (N.Y. 2021)/Assemb. B. 680A, 2021-2022 Reg. Sess. (N.Y. 2021). Notably, there is no requirement that the reasonability of security or foreseeability of harm be industry specific—even though "industry" is likely to be a significant consideration in an enforcer's determination of what constitutes "reasonable."

[234] By "superiorly resourced," I am referring to scientific and medical research projects benefiting from access to more readily accessible data by which to achieve the institution's research goals. New York citizens' resulting enjoyment of these benefits is predicated on NY Privacy Acts' processing requirements rendering the data completely anonymous or unidentifiable.

its parent committee. First, it will ensure that the entity seeking to use biometric data is using such data for its claimed purpose, which must align with the definition and scope of scientific research and the research exemption proposed in Section IV.A and other relevant parts of the NY Privacy Acts. Second, it will ensure that the entity approved to use this biometric data has consistently maintained and properly implemented safeguards to preclude the reidentification of that data by its third-party affiliates or unauthorized entities. Similar to its parent committee, the subcommittee should be responsible for interpreting what constitutes a "reasonable" security measure in a given circumstance, likely considering the industry of the entity that is processing the biometric data.

CONCLUSION

Biometric data is the most sensitive form of data because it is biologically tied and unique to the individual.[235] Nonetheless, biometric data is an invaluable facet of the research that enables progressive scientific, technological, and medical innovation. Because a comprehensive federal data privacy act does not appear to be on the horizon, the torch has been passed to the states to create their own protective regimes. New Yorkers' personal biometric data is not aptly protected, partially because neither the NYPA nor the BPA have matured to the point of becoming a legislative reality. As written, the NY Privacy Acts fail to clearly define research and the boundaries of a sufficient research exemption from mandated erasure. To properly protect New Yorkers' biometric data while realizing the benefits of research, the NY Privacy Acts should adopt a tripartite definition of research from the GDPR, the CCPA, and the CPRA with a reasonable degree of added reverence for the "open science" concept. Finally, the NY Privacy Acts should mandate the imposition of both a data protection agency and a biometric subcommittee that would ensure compliance with the elevated privacy standards required for biometric data, thereby serving as the gatekeepers for research in the Empire State. Without these gatekeepers, New York would be locking up research and throwing away the key.

Eric B. Green[†]

---

[235] BIPA, 740 ILL. COMP. STAT. 14/5(c) (2008).

[†] J.D. Candidate, Brooklyn Law School, 2022; B.S. University of Vermont, Grossman School of Business, 2017. Thank you to Kellie Van Beck, Julia Cummings, Crystal Cummings, and the entire *Brooklyn Law Review* staff for their countless hours dedicated to the writing and editing process. Special thank you to my family, friends, and Michelle, who had my back the entire way.