Ongoing and Emerging Issues in Privacy and Security in a Post COVID-19 Era: An Environmental Scan

A report for the National Committee on Vital and Health Statistics

January 2023

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

This report was prepared under contract by Cason D. Schmit, J.D., Assistant Professor, Department of Health Policy and Management, Texas A&M University School of Public Health

The National Committee on Vital and Health Statistics (NCVHS) serves as the statutory [42 U.S.C.242(k)] public advisory body to the Secretary of the Department of Health and Human Services (HHS) in the areas of health data, standards, statistics, national health information policy, and the Health Insurance Portability and Accountability Act (HIPAA). In that capacity, the Committee provides advice and assistance to HHS and serves as a forum for interaction with relevant private sector groups on a range of health data issues. The Committee is composed of eighteen individuals from the private sector who have distinguished themselves in the fields of health statistics, electronic interchange of health care information, privacy and security of electronic information, population-based public health, purchasing or financing health care services, integrated health information systems, health services research, consumer interests in health information, health data standards, epidemiology, and the provision of health services. Sixteen of the members are appointed by the Secretary of HHS for terms of four years each. Two additional members are selected by Congress. Additional information, including membership roster is available at: https://ncvhs.hhs.gov/

NCVHS Members

Jacki Monson, JD, Chair
Melissa Goldstein, JD, Subcommittee Co-chair*
Valerie Watzlaf, PhD, MPH, RHIA, FAHIMA, Subcommittee Co-chair*
Tammy Banks, MBA
Denise Chrysler, JD*
Jamie Ferguson
Richard W. Landen, MPH, MBA
Denise Love, BSN, MBA
Vickie Mays, PhD, MSPH*
Margaret A. Skurka, MS, RHIA, CCS, FAHIMA
Debra Strickland, MS
Wu Xu, PhD
*Member of the NCVHS Privacy, Confidentiality and Security Subcommittee

Rebecca Hines, MHS
Health Scientist
NCVHS Executive Secretary/Designated Federal Officer (DFO)
National Center for Health Statistics (NCHS), Centers for Disease Control and Prevention (CDC), HHS

Maya Bernstein, JD
Lead Staff to the Subcommittee
Office of Science and Data Policy, Assistant Secretary for Planning and Evaluation (ASPE), HHS

Marietta Squire, NCHS, CDC, HHS
NCVHS Committee Management Specialist

CONTENTS

EXECUTIVE SUMMARY

Information privacy, confidentiality, and security continue to be issues of national importance. In the last four years, there have been substantial developments in law, legal theory, data analytics, privacy preserving technologies, efforts to promote novel and socially beneficial data applications, and public disclosures of concerning data applications.

The National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy, Confidentiality and Security (PCS) requested this environmental scan to better understand recent developments in privacy, confidentiality and security issues in the health, healthcare, and public health sectors.[1] Accordingly, this environmental scan was developed to guide PCS and NCVHS in identifying new major projects to pursue.[1] This report is primarily focused on developments occurring during or after 2018.

PROPOSED AND ENACTED STATE AND FEDERAL PRIVACY LEGISLATION

Nationally, there are intensive efforts to address privacy and security risks in state and federal legislation. At the state level, momentum for new comprehensive privacy legislation is "at an all-time high."[2] Since 2018, five states have adopted new comprehensive privacy laws: California, Colorado, Connecticut, Virginia, and Utah. Four additional states—Michigan, New Jersey, Ohio, and Pennsylvania—have active comprehensive privacy bills under active consideration. Also noteworthy is the Uniform Law Commission's Uniform Personal Data Protection Act, which introduces several innovative privacy provisions.[3] These innovations include a factor-based approach to defining allowable data uses and incorporating a voluntary consensus standard approach to enable the law to adapt to evolutions to data practices over time.

In comparison to state activity, few new federal privacy laws have been adopted. However, dozens of bills have been introduced, and at least one has broad support.[4] The 21st Century Cures Act's regulations defining exceptions to the Act's prohibition of "information blocking" is a notable exception to relative federal inactivity.[5] Nevertheless, Congress has been busy

exploring new federal privacy legislation with over 50 federal privacy bills introduced during the 117th Congress.[4] Of these, the American Data Privacy & Protection Act (ADPPA) is considered the most significant and promising federal comprehensive privacy effort in the past decade.[67] However, there are still significant political challenges to overcome before the ADPPA can become law.[8,9]

NEW PRIVACY AND SECURITY RISKS AND PROMISING POLICIES, PRACTICES AND TECHNOLOGIES

This environmental scan explores two significant new risks to privacy and security: artificial intelligence and law enforcement use of private data. Artificial intelligence has evolved in a largely unregulated space.[10,11] This has created significant alarm due to the growing reliance on these tools across sectors.[12–14] Risks associated with artificial intelligence cross social, health, economic, and political dimensions.[12–20] Notably, artificial intelligence processes can be opaque, making it difficult for consumers to understand risks or difficult for processors to evaluate the unintended effects of their algorithms. In particular, group harms can be pronounced in artificial intelligence applications.[21]

Additionally, multiple high-profile stories have alarmed the public and lawmakers about the scope of law enforcement use of data. These include the use of commercial DNA databases to identify criminal suspects from the DNA of their distant relatives, [22] the criminalization of once legal health procedures (e.g., after the *Dobbs v. Jackson* Supreme Court decision, which overturned a long recognized federal constitutional right to abortion,[23]) as well as law enforcement using commercial surveillance tools to achieve "mass surveillance on a budget."[24]

Despite these challenges, there are many innovations in privacy policies, practices, and technologies. This report describes four primary approaches to contemporary privacy legislation: (1) the consumer protection model, e.g., notice and consent, (2) the data protection approach, similar to the European Union's General Data Protection Regulation (GDPR), (3) the antitrust approach, i.e., focusing oversight on dominant entities, and (4) the information fiduciary approach, i.e., imposing legal duties of confidentiality, care, and loyalty on data controllers.

Similarly, this report describes different approaches to privacy enforcement. Each alternative can be consequential for the effectiveness of a given regulatory framework.[25] These enforcement options include, (1) delegating enforcement authority to a preexisting or newly created agency, (2) enforcement through an individual right of action, (3) deputizing intermediaries to enforce standards and discipline, (4) increasing standards and associated penalties according to the scale of the activity or the size and sophistication of the regulated entity, (5) profit disgorgement, and (6) personal liability for corporate executives.[25]

POTENTIAL PROBLEMS IN GOVERNANCE OF HEALTH INFORMATION

The U.S. privacy framework is often derided as a patchwork of laws.[26–31] This patchwork is both overly complex and under protective. The U.S. legal privacy framework is under protective when its sector-by-sector and jurisdiction-by-jurisdiction approach leaves personal information un(der)-regulated (e.g., commercial data).[32,33] This sectoral approach leads to uneven protections that can be confusing to consumers (e.g., health information stored in a hospital versus health information stored in a fitness-tracking app).[34] The U.S. privacy framework is also overly complex because of inconsistency between jurisdictional approaches. This variability complicates compliance. This is one reason why industry has embraced calls for a national comprehensive privacy law.[35–39] Notably, the U.S. privacy framework might also be considered *over*protective where it restricts popular and socially beneficial data uses.[28] For example, a 2020 national survey of U.S. adults measured privacy preferences, and it identified instances where socially beneficial and popular data uses might be impeded by existing privacy restrictions.[40]

This environmental scan also identifies and explores important and contentious issues in legislative debates. These include (1) defining and regulating sensitive data, (2) preemption of state laws, (3) treatment of existing federal laws, (4) authorizing an individual right of action, and (5) the impact of privacy legislation on healthcare and public health data practices.

In addition, developments in data science, world events, and privacy scholarship necessitate discussion of four additional issues. First, artificial intelligence's anticipated risks and benefits warrant regulatory attention, but it presents a challenging regulatory target.[11] Second, the

COVID-19 response exposed significant challenges and concerns in public health data collection, use, sharing, and governance. Third, de-identification remains a significant issue in part because (1) data science and reidentification methods have seemingly outgrown decade old guidance, and (2) new scholarly thinking on group harms raises concerns about the effect of de-identification methods on groups. Fourth, there is increasing skepticism of the effectiveness of the notice-and-consent model within legal scholarship, which raises questions on the sustained reliance on this approach given available alternatives.

OPPORTUNITIES FOR TIMELY ADVICE FROM NCVHS TO THE HHS SECRETARY REGARDING CONSTRUCTIVE ACTIONS THAT HHS AND OTHER FEDERAL DEPARTMENTS MIGHT TAKE.

This environmental scan identifies four opportunities for timely advice to the HHS Secretary:

1. De-identification remains a critically important issue in privacy. It would be prudent to re-visit the 2017 NCVHS recommendations on deidentification, which remain highly relevant to contemporary issues, in addition to other considerations (e.g., group harms).
2. Recent concerns about law enforcement access to and use of private information raise parallel questions about whether existing law enforcement disclosure exceptions in some privacy laws might enable inappropriate uses. An NCVHS convening could help refine and identify nuance within this area. Some of the issues that could be explored in more detail include narrowing the scope of law enforcement exceptions and imposing data protection requirements on data disclosed for law enforcement purposes (e.g., duties of data minimization or purpose limitation).
3. Artificial intelligence and machine learning tools are reshaping the structures of health care delivery as well as broader social structures, but many existing federal laws do not account for the fundamental difference in the scope and scale of the risks associated with these automated processes. A future NCVHS convening could explore the following issues: (1) standards and requirements for conducting algorithm impact assessments, (2) algorithm transparency requirements or standards, and (3) higher standards, duties, or penalties based on the size and sophistication of the data controller.

4. There are important health implications for the Federal Trade Commission advance notice of proposed rulemaking (ANPRM) on Commercial Surveillance and Data Security. Some unintended consequences could be mitigated by early communication between HHS and FTC to ensure that proposed rules consider the health perspectives and objectives. If FTC promulgates new regulations on commercial surveillance, joint guidance by the FTC and HHS might be needed to ensure that HIPAA covered entities understand their compliance obligations under both laws. A future NCVHS convening could explore whether timely comments or input could inform or assist the FTC rulemaking process and group harm considerations.

I. INTRODUCTION

Information privacy, confidentiality, and security continue to be issues of national importance. However, these are not stagnant issues. Instead, they are issues that evolve in both their scope and effect. Rapid development of information technology, data science, and data analytics continues to strain legal data protection frameworks that change at a much slower pace. World events, like COVID-19, change the context and substance of public discourse, uncovering new applications, questions, and issues.

In response to these challenges, industry members, privacy advocates, legal scholars, researchers, and legislators are continually identifying new issues and exploring potential solutions to an ever-changing new normal. In the last four years alone, there have been substantial developments in law, legal theory, data analytics, privacy preserving technologies, efforts to promote novel and socially beneficial data applications, and public disclosure of concerning data applications. This environmental scan identifies and explores the policy issues surrounding many of these developments; however, it should not be considered a comprehensive review. There are many important issues that are not fully explored here.

Section II of this environmental scan provides an overview of significant changes in the privacy legal landscape and describes state and federal laws that have been enacted or proposed. Section III of this report identifies new privacy and security risks, focusing predominantly on artificial intelligence and law enforcement access to and use of private information. Section IV describes several promising policies and practices on these issues, including different approaches to data privacy and different enforcement options. Section V explores several challenges in the governance of health information, including existing gaps in legal protections, contentious issues in legislative debates, protecting data while enabling socially beneficial uses, and de-identification. Finally, Section VI provides four opportunities where timely advice from the National Committee on Vital and Health Statistics (NCVHS) could enable constructive actions on issues of data privacy, confidentiality, and security from federal agencies.

A. BACKGROUND

NCVHS is a statutory advisory body for the Secretary of the U.S. Department of Health and Human Services (HHS).[41] In this capacity, NCVHS assists and advises the Secretary on issues concerning health data, privacy, standards, statistical methods, and national health information policy. NCVHS also assists and advises the Department in the implementation of the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA).[41]

The NCVHS Strategic Plan establishes four strategic goals:

1. "Improve data usability and analytic capabilities to sustain continuous improvement in health and well-being for all."
2. "Accelerate the adoption of standards to achieve the purposes of safety, effectiveness, efficiency, privacy, security and interoperability of health data and systems."
3. "Expand appropriate access and use of data while ensuring relevant safeguards."
4. "Improve health information and data policy by taking the long view."[42]

Within NCVHS, the Subcommittee on Privacy, Confidentiality and Security (PCS) monitors developments in health information privacy, confidentiality, and security, and identifies issues and opportunities for further investigation. In addition, PCS makes recommendations to NCVHS and assists HHS in its administration of the HIPAA privacy and security provisions.

The NCVHS PCS Subcommittee requested this environmental scan to better understand recent developments in privacy, confidentiality and security issues in the health, healthcare, and public health sectors.[1] Accordingly, this environmental scan was developed to guide PCS and NCVHS in identifying new major projects to pursue.[1] This report is primarily focused on developments occurring during or after 2018.

II. SIGNIFICANT CHANGES IN THE PRIVACY LANDSCAPE SINCE 2018

Nationally, there are intensive efforts to address privacy and security risks in state and federal legislation. At the state level, momentum for new comprehensive privacy legislation is "at an all-time high."[2] Although few new federal privacy laws that have been adopted at the federal level, dozens of bills have been introduced, and at least one has broad support.[4] This section describes the laws that have been adopted and reviews innovative and noteworthy elements of proposed legislation at both the state and federal level.

A. STATE POLICY DEVELOPMENTS

1. STATE PRIVACY LAWS ENACTED

Since 2018, five states have adopted new comprehensive privacy laws: California, Colorado, Connecticut, Virginia, and Utah. This section summarizes the enacted laws in those states.

A) CALIFORNIA

California has adopted or amended its privacy framework several times since 2018. This section reviews those developments with a focus on California's comprehensive privacy framework.

(1) CALIFORNIA PRIVACY RIGHTS ACT

California adopted the California Consumer Privacy Act in 2018.[43] Since then, it has been amended twice by the state legislature and a third time by referendum in 2020.[44–46] The revised Act, titled the California Privacy Rights Act of 2020 (CPRA), becomes operative on January 1, 2023.[46] This section describes the CPRA as it will become effective in 2023.

CPRA applies to businesses defined as those "organized or operated for the profit or financial benefit of its shareholders or other owners" that have annual gross revenues over $25 million or "annually buys, sells, or shares the personal information of 100,000 or more consumers."[47] However, CPRA will also apply to smaller businesses if it "[d]erives 50 percent or more of its annual revenues from selling or sharing consumers' personal information." Non-profits do not appear to be covered by CPRA.[47] CPRA also has several large exemptions where controllers,

processors, or information are covered by other major federal laws including HIPAA, Gramm-Leach-Bliley Act (GLBA), Driver's Privacy Protection Act (DPPA) and the Fair Credit Reporting Act (FCRA).[48]

CPRA protects personal information, defined as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[49] HIPAA deidentified data and data subject to the Common Rule regulations for human subjects research are exempted from CPRA.[50]

CPRA provides additional protections for sensitive personal information, which includes information on government identifying numbers, log-in information, precise geolocation, race/ethnicity, religious or philosophical beliefs, union membership, genetic information, personal communications, biometrics, health, sexual orientation, and sexual behavior.[51] CPRA provides additional individual rights to restrict uses of sensitive information, subject to extensive and complex exceptions,[52] and there is a specific means for consumers to opt-out of the distribution of their sensitive information.[53]

CPRA permits data controllers and processors to engage in data practices that are reasonable and proportionate "to achieve the purposes for which the personal information was collected or processed," or for another disclosed compatible purpose.[54] However, CPRA grants consumers an "opt-out right" that permits the consumer to direct business not to share or sell their personal information.[55] In addition, CPRA imposes a duty of care "to implement and maintain reasonable security procedures and practices appropriate to the nature of the information."[56]

CPRA enables enforcement through a private right of action or through state enforcement by the California Privacy Protection Agency. In a private action, litigants can seek injunctive relief, actual damages, or statutory damages between $100 and $750 per consumer per incident.[56] The California Privacy Protection Agency can seek penalties of $2,500 per incident.[56,57]

(2) THE CALIFORNIA AGE-APPROPRIATE DESIGN CODE ACT

On September 15, 2022, California Governor Gavin Newsom signed the California Age-Appropriate Design Code Act.[58] Unfortunately, a detailed analysis of this new law was not completed due to its recency. However, the new law bars technology companies from "profiling children or using personal information in ways that could harm children physically or mentally."[59] According to the Associated Press, the new law requires businesses that provide services attractive to children "follow age-appropriate design code principles aimed at keeping children safe," and companies must submit "data protection impact assessments" to the state attorney general before offering new services.[59]

B) COLORADO

On July 7, 2021, Governor Jared Polis signed the Colorado Privacy Act (CPA), which takes effect July 1, 2023.[60] CPA applies to Colorado businesses or businesses that target Colorado residents that either (1) annually control or process data on at least 100,000 persons or (2) earn revenue (or receive a discount) from the sale of personal data and process or control data on at least 25,000 persons.[61] Unlike California, there is no provision for small businesses in the CPA.[61]

CPA imposes several duties on data controllers. These include duties of (1) transparency[62]—"accessible, clear, and meaningful privacy notice"—(2) purpose specification,[63] (3) data minimization,[64] (4) avoidance of secondary uses[65]—no processing of personal data that are not "reasonably necessary to or compatible with the specified purposes" absent consent—(5) care in implementing appropriate security, (6) avoidance of unlawful discrimination,[66] and (7) consent for processing sensitive data.[67] CPA generally does not require consent for collecting or processing data that is reasonably necessary for or compatible with the purpose of the data collection.[65] Colorado provides a right to opt out of "(i) targeted advertising, (ii) the sale of personal data, or (iii) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the consumer."[68]

The CPA provides additional protections for sensitive data, which is defined to include information on race/ethnicity, religious beliefs, mental/physical health, sexual orientation, sexual behavior, citizenship, genetics or biometric data for identification, and data on a known

child.[69] Colorado requires consent for data practices using sensitive data.[67] Additionally, CPA requires that controllers and processors that process sensitive data perform a "data protection assessment."[70]

CPA has an extensive list of exclusions and exceptions.[61] For example, CPA broadly excludes certain data covered by major federal laws from its scope, including data protected by HIPAA, GLBA, 42 C.F.R. Part 2, DPPA, Children's Online Privacy Protection Act (COPPA), and Family Educational Rights and Privacy Act (FERPA). [61] CPA also exempts research and some public health activities from its provisions.[71]

CPA authorizes the state attorney general and district attorneys to bring enforcement actions. The available remedies are the same as state deceptive trade practices law.[72]

C) CONNECTICUT

On May 5, 2022, Connecticut became the fifth state to adopt a comprehensive privacy law when Governor Ned Lamont signed the Connecticut Data Privacy Act (CDPA). The Act protects personal data defined as "any information that is linked or reasonably linkable to an identified or identifiable individual" but excluding deidentified data and publicly available information.[73] CDPA applies to businesses within the state or businesses that target its residents that either (1) control or process data on 100,000 consumers (excluding data processing solely for payment transactions), or (2) control or process data on 25,000 consumers and derived at least 25% of their gross revenue from the sale personal data.[74] However, the CDPA has a long list of exemptions for entities and data types. The entity exclusions include (1) government entities, (2) nonprofits, (3) higher education institution, (4) registered national securities associations, (5) entities governed by GLBA, and (6) HIPAA covered entities and business associates. Excluded data types include (1) health and patient information subject to various federal laws, (2) data subject to regulations for human subjects research protections, (3) information used for public health activities and purposes, (4) consumer credit information subject to FCRA, (5) data subject to the DPPA, (6) FERPA data, (7) data subject to the Farm Credit Act, and (8) employment data.[74]

CDPA establishes several consumer rights.[75] These rights include a right to (1) confirm data processing by a controller, (2) correction of inaccurate data, (3) deletion of personal information, (4) data portability, and (5) opt-out of data processing for targeted advertising or the sale of personal data. The Act permits consumers to designate an authorized agent to exercise these rights. CDPA provides substantial flexibility for this designation by permitting agent designation "by way of… a technology including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating such consumer's intent to opt out of such processing."[76]

The Act imposes several obligations on controllers.[77] First, controllers are required to limit data collection "to what is adequate, relevant and reasonably necessary" for disclosed purposes (i.e., data minimization). Second, controllers cannot "process personal data for purposes that are neither reasonably necessary to, nor compatible with," disclosed purposes (i.e., purpose limitation). Third, controllers must "establish, implement and maintain reasonable administrative, technical and physical data security practices" that are appropriate for the data type. Fourth, the Act prohibits unlawful discrimination. Fifth, controllers must provide an "effective mechanism" for consent revocation "at least as easy as the mechanism by which the consumer provided… consent."[77] Sixth, controllers have additional restrictions for data on children between 13 and 16 years of age, including prohibitions on targeted advertising, and sale of personal data. Seventh, the Act provides specific privacy notice requirements for controllers. Eighth, controllers are required to conduct and document data protection assessments for each processing activity that "presents a heightened risk of harm to a consumer,"[78] specifically including targeted advertising, sales of personal data, and profiling that presents a "reasonably foreseeable risk." Additionally, controllers are prohibited from discriminating against consumers that exercise their CDPA rights (excepting bona fide loyalty programs).[77] CDPA also establishes relational and contractual obligations between controllers and processors.[79]

CDPA has additional protections for sensitive data.[77] Specifically, CDPA requires controllers to obtain consent prior to processing these sensitive data or compliance with COPPA where the

data pertain to a known child.[77] The Act defines “sensitive data" to include data on (1) race/ethnicity, (2) religious beliefs, (3) mental/physical health condition or diagnosis, (4) sex life, (5) sexual orientation, (6) citizenship/immigration status, (7) genetic or biometric data for identification purposes, (8) personal data collected from a known child, and (9) precise geolocation data.[73]

The state attorney general has the exclusive authority to enforce the CDPA.[80]

D) UTAH

On March 24, 2022, the Utah Consumer Privacy Act (UCPA) was signed into law.[81] UCPA protects personal data defined as “information that is linked or reasonably linkable to an identified individual or an identifiable individual.”[82] Deidentified data, aggregated data, and publicly available information are specifically excluded from the definition of “personal data.” UCPA regulates data controllers and processors that conduct business in Utah or targets its residents as consumers of products or services.[83] However, it applies only to controllers or processors that (1) have annual revenues of at least $25 million, (2) control or process data on at least 100,000 consumers, or (3) derived over 50% of the entity’s gross revenue from the sale of personal data and control or process personal data on at least 25,000 persons. The Act has an extensive list of broad exemptions, including exemptions for (1) governments, (2) tribes, (3) higher education institutions, (4) non-profits, (5) HIPAA covered entities and business associates, (6) HIPAA protected health information, (7) information governed by 42 CFR Part 2, (8) human subjects research activities and data, (9) activities of consumer reporting agencies, (10) entities governed by GLBA, (11) data governed by DPPA, (12) data governed by FERPA, and (13) employment data.

UCPA establishes several consumer rights. These rights include rights to (1) confirmation of data processing, (2) data access, (3) deletion of provided data, (4) portability, and (5) opt out of targeted advertising or the sale of personal data.[82] The Act establishes processes for consumers to exercise these rights and for the controller’s response to consumer requests.[83,84]

In addition, UCPA imposes obligations on processors and controllers.[85] These obligations include contractual requirements between controllers and processors and security measures.[86]

The Act also requires that controllers provide "a reasonably accessible and clear privacy notice."[86] The Act creates some limited restrictions on discrimination. For example, if a consumer exercises a right under the Act, then a controller cannot deny a good or service, charge a different price, or provide products or services with a different level of quality. However, controllers may discriminate if consumers opt-out of targeted advertising or do not participate in a bona fide loyalty program.[87]

The Act has specific requirements for data defined as sensitive and data pertaining to a known child. "Sensitive data" are defined to include data on (1) race/ethnicity, (2) religious beliefs, (3) sexual orientation, (4) citizenship/immigration status, (5) mental/physical health, (6) genetic or biometric data for identification purposes, and (7) specific geolocation data.[82] Controllers that process sensitive data must provide consumers with a clear notice and an opportunity to opt-out of data processing. This right to opt-out of sensitive data processing is broader than the consumer right to opt-out defined in Section 202, which is limited to targeted advertising and sale of personal data. UCPA requires compliance with COPPA for processing data on a known child.

UCPA grants investigation authority for violations of the Act to the Division of Consumer Protection within the state Department of Commerce.[88] However, the state attorney general has the exclusive enforcement authority for violations of the UCPA.[89] A newly created Consumer Privacy Restricted Account is funded through UCPA civil enforcement actions, and its funds can be used for future enforcement activities.[90] Private rights of action are expressly prohibited by the Act.[91]

E) VIRGINIA

Virginia adopted the Consumer Data Protection Act (VCDPA) on March 2, 2021, with an effective date of January 1, 2023.[92] VCDPA applies to "persons that conduct business" in Virginia or target its residents as customers.[93] However, VCDPA is limited to larger controllers and processors, defined as those that "control or process personal data of at least 100,000 consumers or... control or process personal data of at least 25,000 consumers and derive over 50 percent of gross revenue from the sale of personal data").[94]

VCDPA broadly exempts large categories of entities and data.[95] Excluded entities include government entities, financial institutions subject to GLBA, HIPAA covered entities, non-profits, and institutions of higher education. Exempted data include, health records, data governed by the Common Rule regulations for human subjects research, data governed by FERPA, consumer credit information governed by FCRA, personal data subject to the Farm Credit Act, employment data, and data for authorized public health activities.[95]

VCDPA enumerates several consumer rights. These rights include rights to (1) confirm data processing, (2) data access, (3) data correction, (4) data deletion, (5) data portability, and (6) opting out of targeted advertising, the sale of personal data, and profiling for decisions with significant consumer impacts.[96]

VCDPA also imposes responsibilities and duties for data controllers. These responsibilities include (1) limiting data collection to what is "adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed," (2) not processing "personal data for purposes that are neither reasonably necessary to nor compatible" with disclosed purposes, (3) establishing appropriate administrative, technical and physical security, (4) avoidance of unlawful discrimination, (5) not processing sensitive personal data without consumer consent, and (6) transparency and disclosure of data practices in a privacy notice.[97]

Virginia does not require consent for "collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the purposes for which such data is processed, as disclosed to the consumer" or for processing for those purposes or for "compatible" purposes. with them.[97] However, VCDPA contains additional protections for sensitive personal data. Sensitive data are defined to include data on (1) race/ethnicity, (2) religious beliefs, (3) mental/physical health, (4) sexual orientation, (5) citizenship/immigration status, (6) genetic or biometric data used for identification, (7) precise geolocation, and (8) data on a known child.[98] Virginia requires consent for any data practice involving sensitive data.[99] Additionally, a "data protection assessment" is required if sensitive data are processed.[100]

VCDPA authorizes only the state attorney general to enforce its provisions. VCDPA authorizes injunctive relief, civil penalties up to $7,500 per violation, or both.[101]

2. OVERVIEW OF STATE PRIVACY LAWS UNDER CONSIDERATION

As of August 2022, the International Association of Privacy Professionals (IAPP) identified active privacy bills in 4 states: Michigan, New Jersey, Ohio, and Pennsylvania.[2] In addition to these active bills, the IAPP identified 49 "inactive" bills in 23 additional states (AK, AZ, FL, GA, HI, IN, IA, KY, LA, ME, MD, MA, MN, MS, NE, NY, NC, OK, RI, VT, WA, WV, and WI).[2] This volume of legislation suggests that comprehensive privacy legislation remains an important issue across many U.S. jurisdictions. This section reviews the privacy bills that were under active consideration as of August 2022.

A) MICHIGAN

The Michigan Consumer Privacy Act (CPA; HB 5989) is the sole active bill in the state.[102] CPA broadly protects "personal data" and applies to large businesses that operate in Michigan or target its residents. Businesses would only be subject to CPA if they either control or process data on 100,000 individuals or if they control or process data on $25,000 individuals and derive at least 50% of their gross revenue from the sale of personal data.[103]

CPA establishes new consumer rights pertaining to their data.[104] These rights include (1) rights of transparency (i.e., for data collection, disclosure, and sale), (2) a right to opt-out of certain activities (i.e., sale of data, targeted advertising, profiling), (3) a right of access to their personal data, (4) a right to request personal data deletion, (5) a right to correct incorrect personal data, and (6) a right of non-discrimination for exercising privacy rights.

CPA largely follows a data protection approach that imposes limitations and obligations on data controllers (see Section IV.A below). For example, the collection of personal data is limited "to what is adequate, relevant, and reasonably necessary in relation to the purposes for which the personal data are processed."[105] However, the bill permits greater personal data collection with consumer consent. The bill also imposes obligations to "[e]stablish, implement, and maintain

reasonable administrative, technical, and physical data security practices" that are appropriate to the volume of data and obligations to conduct data protection assessments.[106]

CPA also requires consumers to provide consent prior to processing sensitive data.[105] Sensitive data are defined to include data on (1) race/ethnicity, (2) mental/physical health, (3) sexual, orientation, (4) citizenship/immigration status, (5) genetic or biometric data for commercial uses, (6) information pertaining to a known child, and (7) precise geolocation.[107]

CPA currently grants the state attorney general exclusive enforcement authority.[108]

B) NEW JERSEY

Currently there are three active privacy bills in New Jersey. One bill is comprehensive in scope (i.e., A505), and two bills are limited to commercial internet websites and online services (i.e., S332 and A1971). This section will summarize only the comprehensive privacy bill.

The New Jersey Disclosure and Accountability Transparency Act (NJ DaTA; A505)[109] broadly regulates the collection and processing of consumers' personally identifiable information[110] by data controllers and processors. Unlike other privacy bills discussed here, there are no provisions that limit the applications of NJ DaTA to larger controllers. However, NJ DaTA excludes several large categories of entities and types of data processing.[111] These exclusions include HIPAA-covered entities, financial institutions governed by GLBA, and processing by a consumer reporting agency that is subject to the FCRA.

NJ DaTA establishes several consumer data rights.[112] These rights include rights to (1) opt-in to data collection, (2) lawful, fair, transparent data processing, (3) limited data collection, (4) minimization of personally identifiable data, (5) data accuracy and to request correction, (6) data security, (7) data access, and (8) objection to data processing (controllers have a right of rebuttal).

Additionally, NJ DaTA imposes certain obligations on data controllers. Controllers must provide consumers with a "concise, transparent, intelligible, and easily accessible" notice describing the

nature of the data collection and data uses.[113] There are also sections pertaining to data security,[114] breach notification, and conducting privacy impact assessments.[115]

Generally, NJ DaTA only permits data processing in six situations: (1) the consumer has provided affirmative (opt-in) consent, (2) the processing is necessary to satisfy contractual obligations with the consumer, (3) to comply with legal obligations, (4) to protect the "vital interests" of a person, (5) to perform a task in the public interest, or (6) to further legitimate interests that are not outweighed by individual rights or interests.[116]

Sensitive information is subject to a general processing prohibition under NJ DaTA, unless an exception applies.[117] Under NJ DaTA, sensitive information is defined to include information pertaining to (1) race/ethnicity, (2) political opinion, (3) religious/philosophical belief, (4) trade union membership, (5) biometric data used for identification, (6) health information, (7) and sexual history or orientation. Despite the general prohibition, controllers can process sensitive information if a consumer provides consent to processing the sensitive information, or if the processing is for preventive or occupational medicine, public health activities, or archiving purposes in the public, scientific, or historical interest.

Enforcement authority for compliance with NJ DaTA is not expressly stated in the act. However, The Division of Consumer Affairs in the Department of Law and Public Safety has rulemaking authority for the NJ DaTA, and the state attorney general has authority to appoint (with consultation) the executive director of the Office of Data Protection and Responsible Use within that Division.

C) OHIO

The Ohio Personal Privacy Act (PPA; HB 376) is the sole comprehensive privacy bill active in the Ohio legislature.[118] PPA broadly applies to personal data that is reasonably linkable to an identifiable consumer and processed by a business for a commercial purpose. It applies to businesses, including non-profits, that operate within Ohio or target its residents for goods or services.[119] Businesses are defined to include non-profits but exclude governments. In addition, PPA limits its coverage to businesses that either (1) have revenues over $25 million, (2) annually

controls or processes personal data on 100,000 consumers, or (3) derive 50% of revenue from data sales, and process or control personal data on 25,000 or more consumers.

In addition, PPA has an extensive list of exclusions, which include exclusions of certain entities, data types, and other activities. Entities excluded from the PPA include government entities, GLBA-governed financial institutions, HIPAA covered entities, and higher education institutions. There are broad PPA exemptions for "business to business transactions" and insurance activities. Health-related data are broadly excluded from the PPA, including separate exclusions for data protected by HIPAA, health records, patient identifying information, documents relating to the Health Care Quality Improvement Act, and information used only for public health activities. Other data exemptions include human subjects research data, data governed by the COPPA, consumer credit information governed by FCRA, data protected by FERPA, driver's license data, and employment data. The PPA also broadly permits covered businesses to conduct research, cooperate with law enforcement, exercise, or defend legal claims, and take immediate steps to protect life. In additional to the above exclusions, the PPA broadly states that many PPA consumer rights do not apply to "pseudonymous data."[119]

PPA establishes several consumer rights.[120] These rights include rights to (1) notice of the personal data that a business collects, (2) data access, (3) data portability, (4) correct inaccuracies, (5) data deletion, (6) opt-out of the sale of personal data or targeted advertising, and (7) non-discrimination for exercising privacy rights.

In addition to establishing these privacy rights, PPA regulates the contractual obligations between data controllers and processors.[121] These regulations include specific governance practices for the data subject to the contract.

PPA gives the state attorney general the exclusive enforcement authority.[122] The consequences for PPA violations include injunctive relief civil penalties.

D) PENNSYLVANIA

Pennsylvania currently has three active comprehensive privacy bills. Two separate bills share the same title, Consumer Data Privacy Act (HB 1126 and HB 2202), and the third bill is titled the Consumer Data Protection Act (HB 2257).[123–125]

(1) CONSUMER DATA PRIVACY ACT (HB 1126)

The first Consumer Data Privacy Act (HB 1126) applies to for profit entities that conduct business in Pennsylvania that either (1) have annual gross revenues of over $10,000,000; (2) annually buys, receives, sells, or shares personal information of at least 50,000 persons; or (3) earns at least 50% of annual revenue from the sale of personal information.[126]

HB 1126 protects personal information, which is defined as non-publicly available, identifiable information. The bill uses a long non-exhaustive list of identifier examples covered under the law. The examples of protected information include education (not FERPA) data, internet activity, biometrics, geolocation, and employment data.[126]

HB 1126 creates several consumer data rights.[127] Consumer rights under HB 1126 include rights to (1) transparency for data collected, sold, or disclosed, (2) requests additional disclosures from businesses, (3) opt-out of the sale of personal information, (4) data access, and (5) non-discrimination for exercising privacy rights. HB 1126 provides specific protections for individuals under the age of 16. There are exemptions for deidentified or aggregate information.

Individuals and the state attorney general are empowered to bring civil actions to enforce violations of HB 1126.[128] The bill also permits the attorney general to provide advisory opinions.[129]

(2) CONSUMER DATA PRIVACY ACT (HB 2202)

The second Consumer Data Privacy Act (HB 2202) applies to for profit entities that conduct business in Pennsylvania that either (1) have annual gross revenues of over $20,000,000; (2) annually buys, receives, sells, or shares personal information of at least 100,000 persons; or (3) earns at least 50% of annual revenue from the sale of personal information.[130] HB 2202 also applies to the service providers of businesses.

As compared to HB 1126, HB 2202 provides a simplified definition of personal information, including only information that is identifiable or can be reasonably linked to an individual consumer, household, or consumer device.[130] HB 2202 excludes information from government records and information that is deidentified or aggregated.

HB 2202 establishes several consumer rights.[131] These rights include the right to (1) transparency of data processing, sale of personal data, and targeted advertising, (2) opt-out of targeted advertising, sale of personal data, and significant profiling decisions, (3) data access, (4) data correction, (5) deletion of personal information, and (6) data portability.[131]

HB 2202 imposes several obligations and duties on businesses.[132] There are numerous duties described in the bill. These include (1) a duty of care to "implement and maintain reasonable security procedures and practices"[133] (2) duties of data minimization,[134] (3) a duty to avoid secondary uses that are not necessary nor compatible with the primary data use (unless the consumer provides consent),[135] and (4) duties of non-discrimination for exercising privacy rights and including compliance with federal and state law.[136] Additionally, HB 2202 details specific requirements for consumer privacy notices and provides specific restrictions on processing information on someone less than 16 years old.[137,138] In addition, HB 2202 imposes obligations on service providers, including confidentiality and security requirements as well as contractual obligations with covered businesses.[139]

HB 2202 contains several broad exceptions that permit businesses to broadly conduct certain activities.[140] These exceptions include compliance with legal requirements, cooperation with law enforcement, to collect, use, retain, sell, or disclose deidentified information, to take immediate steps to protect interests essential to life, and to conduct human subjects research (with some restrictions).

HB 2202 gives the attorney general rulemaking authority and authorizes the attorney general to provide advisory opinions. Violations of HB 2202 would be considered violations of the Unfair Trade Practices and Consumer Protection Law and are eligible for civil penalties and injunctive relief.[141]

(3) CONSUMER DATA PROTECTION ACT (HB 2257)

The Consumer Data Protection Act (CDPA) is the most substantive of the three Pennsylvanian bills (i.e., it is longer than the other two bills combined).[123] Most of the CDPA restrictions and responsibilities apply to businesses that conduct business in Pennsylvania that either (1) annually control or process personal information on at least 100,000 individuals or (2) annually control or process data on 25,000 individuals and derive 50% or more of annual revenue from sale of personal information.[142]

CDPA has several broad exclusions for certain entities and information types.[143,144] The entity exclusions include government entities, financial institutions governed by GLBA, HIPAA covered entities, non-profits, and higher education institutions.[143] The information type exclusions include several categories of health data, data from human subjects research, information used only for public health activities, consumer credit information, motor vehicle records, education records covered by FERPA, employment data, and information regulated by the COPPA.[144]

CDPA provides two additional classifications of data: "identifiable private information" and "sensitive data." "Identifiable private information" is information that includes at least a first initial and last name in addition to enumerated other types of information (e.g., SSI, driver's' license number, passport number, taxpayer ID, medical information, biometric data, financial account information). "Sensitive data" is defined to include information on (1) race/ethnicity, (2) religious beliefs, (3) mental/physical health, (4) sexual orientation, (5) gender identity, (6) citizenship/immigration status, (7) genetic/biometric data for identification, (8) information on minors, and (9) geolocation.[145]

The bill provides several consumer rights.[146] These rights include a right to (1) confirm personal data processing, (2) data correction, (3) data deletion, (4) data access and portability, and (5) opt-out for targeted advertising, sale of personal data, and profiling for significant decisions.

CDPA generally prohibits any data processing that is not "expressly listed" in the bill or otherwise permitted by the Act.[147] Additionally, controllers must limit data collection to what is necessary, proportionate, and compatible with permissible and disclosed purposes. CDPA

requires controllers to implement reasonable security practices, and expressly prohibits unlawful data processing, discriminating against persons for exercising their privacy rights, or processing sensitive data without an individual's consent.

Additionally, CDPA imposes responsibilities and obligations on businesses and data processors. Businesses are responsible for making a privacy notice available that includes disclosures of sale of personal information and advertising. CDPA requires processors to follow data controller instructions, implement technical, organizational, and security measures, and abide by certain contractual requirements. Data controllers are responsible for conducting data protection assessments that weigh relevant benefits and risks, which may be subpoenaed by the state attorney general.[148]

CDPA provides several exceptions to its restrictions. These include compliance with legal requirements, cooperation with law enforcement, to take immediate steps to protect interests essential to life or safety, and to conduct scientific or product/service development research (with some restrictions). Notably, CDPA consumer rights do not apply to pseudonymized data.

The state attorney general is empowered to enforce the provisions of the Act.[149,150] The bill also establishes a Consumer Privacy Fund, funded through enforcement, where deposited funds can be used to support enforcement.[151]

3. OTHER STATE LAWS

A) UNIFORM PERSONAL DATA PROTECTION ACT

The Uniform Law Commissioners (ULC) approved their draft Uniform Personal Data Practices Act (UPDPA) in July 2021.[3] As model legislation, the ULC has made the UPDPA available to all U.S. state and territorial legislatures.[3] Since release, it has been introduced in three U.S. jurisdictions (DC, NE, OK). UPDPA applies to any person or legal entity that is a controller or processor of personal data. It is restricted to controllers or processors that conduct business in the adopting state or direct products or services to the state's residents.[152] UPDPA excludes government entities, but its coverage of non-profits depends on state determinations on the legal meaning of "conducting business."[153] Like many of the state laws above, the UPDPA has

size thresholds for regulated entities, but permits states flexibility to determine specific thresholds. Notably, the UPDPA will apply to controllers or processors *of any size* if they engage in "incompatible data practices" (see discuion below).[152] UPDPA's protects personal data that relate to a data subject. Deidentified data, publicly available information, and employment data are excluded from UPDPA.[154]

UPDPA has different rules for three categories of data practices: compatible, incompatible, and prohibited. UPDPA allows controllers and processors to engage in compatible data practices without a data subject's consent.[155] Data subjects must be given an opportunity to opt-out of incompatible data practices[156] unless the data practice involves sensitive information, in which case opt-in consent is required. Prohibited data practices are never permitted.[157]

UPDPA has received criticism for being overly business-friendly.[158] Thus, prospects of its adoption remain dim. However, it is worth mentioning that UPDPA contains at least three innovations that have not been widely adopted in U.S. privacy laws.

First, UPDPA incorporates a factor-test for determining whether a data practice qualifies as a "compatible" practice (i.e., no consent required). The factors are: "(1) the data subject's relationship with the controller; (2) the type of transaction in which the personal data was collected; (3) the type and nature of the personal data that would be processed; (4) the risk of a negative consequence on the data subject by the use or disclosure of the personal data; (5) the effectiveness of a safeguard against unauthorized use or disclosure of the personal data; and (6) the extent to which the practice advances the economic, health, or other interests of the data subject." These factors present potential benefit and risks. The factors introduce flexibility into the regulatory regime, which can benefit rapidly evolving technologies like big data. [28,159] However, the flexibility could also be (ab)used by data controllers and processors to justify dubious data practices.[28]

Second, UPDPA expressly prohibits some data practices.[157] The express prohibition of some data practices is a departure from the consumer-centric approach of many U.S. data privacy laws where a consumer's consent theoretically permits all data practices. Notably, however,

UPDPA defines prohibited data practices somewhat narrowly. Some prohibited data practices include reidentifying de-identified data and engaging in a data process that requires consent without obtaining consent.

Finally, UPDPA permits a data practice to become a "compatible" data practice (i.e., no consent required) through a voluntary consensus standard (VCS) process.[155,160] The VCS process is a significant innovation of the UPDPA. A VCS is a formal standard that has been developed through a multistakeholder process—including industry, consumer, and public interests—and recognized by the state attorney general. The VCS process permits the regulatory framework to adapt to the evolving state of data practices without requiring lengthy legislative or regulatory processes.

B) STATE REGULATING AI AND BIOMETRIC DATA PROTECTION LAWS

Several states have introduced laws addressing specific data or data practices. For example, laws regulating AI have been enacted in Alabama, Colorado, and Illinois, and laws governing the use of biometric data have been enacted in Illinois, Texas, and Washington.[161]

B. FEDERAL POLICY DEVELOPMENTS

1. FEDERAL LAWS ENACTED

A) 21ST CENTURY CURES ACT

In 2016 Congress passed the 21st Century Cures Act. Among other things, the Act makes "Information blocking" illegal. The Act defines information blocking broadly as a practice that "is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." This law was a reaction against many business practices that were impeding consumer-friendly or socially beneficial uses of electronic health information, which were anticipated—but incompletely realized—from the 2009 HITECH Act meaningful use incentive program.[162,163] The Act specifically described three general practices that constitute illegal information blocking. Those practices described in the Act are:

1. "practices that restrict authorized access, exchange, or use under applicable State or Federal law of such information for treatment and other permitted purposes"
2. "implementing health information technology in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using electronic health information," and
3. "implementing health information technology in ways that are likely to—
    a. restrict the access, exchange, or use of electronic health information with respect to exporting complete information sets or in transitioning between health information technology systems; or
    b. "lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use."

Recognizing that this definition is quite broad, Congress authorized HHS to promulgate regulations to identify specific practices that should be exempt from the prohibitions of illegal information blocking. In 2020, HHS finalized its information blocking exceptions. These exceptions include practices that relate to (1) preventing harm, (2) protecting privacy, (3) protecting the security of electronic health information, (4) infeasible requests, (5) health IT implementations to maintain or improve performance, (6) limitations on certain content or the manner of producing electronic health information, (7) recovering reasonable costs, and (8) licensing.[5,164] Each of these exceptions have detailed regulatory requirements and conditions.

These information blocking provisions within 21st Century Cures Act aims to free data from restrictive business practices, but there are important privacy implications. For example, the information blocking prohibition might help a person centralize and control their health information from various providers in a Personal Health Record application; however, the application might not be a HIPAA covered entity. Consequently, the robust privacy and security protections that applied to the information in the doctor's office would be gone once the information is imported into the non-HIPAA covered application. Current federal efforts to adopt a comprehensive data protection law might address this example.

2. FEDERAL PRIVACY LAWS UNDER CONSIDERATION

A) AMERICAN DATA PRIVACY AND PROTECTION ACT

In July 2022, the American Data Privacy & Protection Act (ADPPA) passed the full House Energy and Commerce Committee.[7] Although ADPPA is considered the most significant federal comprehensive privacy effort in the past decade,[6] Speaker Pelosi announced that she cannot support the bill's preemption of the substantive protections in state privacy laws like California's.[8,9]

ADPPA regulates data collection and processing by private sector entities, including both businesses and non-profits. Government entities and their service providers are excluded as ADPPA covered entities, but they might face some restrictions under the current bill as "third parties."[165,166] Entities regulated by HIPAA, GLBA, FERPA, the Genetic Information Nondiscrimination Act (GINA), 42 C.F.R. Part 2, and other federal privacy and data security laws are also covered by ADPPA, but they are deemed compliant for ADPPA purposes if they are compliant with their applicable sector-specific laws.[167]

ADPPA draws on data protection principles (see Section IV.A below). For example, ADPPA incorporates principles of data minimization and purpose limitations that are central to the European Union's General Data Protection Regulation (GDPR). The current list of permissible purposes under the ADPPA include purposes necessary to "provide or maintain a specific product or service requested by the individual to whom the data pertains," as well as compliance with legal obligations, public safety incidents, and for public interest scientific research.[168] There is no express public health permissible purpose.[9] ADPPA imposes a variety of duties to provide consumer transparency, access, and control.[169]

The draft ADPPA currently restricts the collection and use of sensitive data to what is "strictly necessary to provide . . . a product or service requested by the individual," and it must be for a permissible purpose.[170] Generally, sensitive data can be transferred only with the affirmative express consent of the individual.[170] ADPPA defines sensitive data as data including (1) physical/mental health, (2) financial information, (3) biometric data, (4) genetic information, (5) sexual behavior data, and (6) data on minors.[170,171]

ADPPA has a variety of enforcement mechanisms. ADPPA authorizes enforcement by FTC and state Attorney General enforcement.[167,172] Additionally, it establishes individual and class action remedies for compensatory damages and attorneys' fees.[173]

The ADPPA establishes rigorous requirements for de-identification.[174] Notably, the data de-identification standards under HIPAA are substantively different HIPAA. Consequently, it is unclear how these two standards would interact in practice. For example, it is unclear whether data de-identified under HIPAA would remain satisfactorily de-identified if transferred to an entity separately regulated under the ADPPA de-identification standard.[9,174,175]

ADPPA's preemption provisions are the most politically controversial feature of the bill.[8,176] Currently, ADPPA would preempt recently passed state laws addressing general data practices in the private sector.[9] It does not, however, preempt other state laws, including those that "address health information," or "pertain to public health activities, reporting, data or services."[177]

B) FTC ADVANCE NOTICE OF PROPOSED RULEMAKING ON "COMMERCIAL SURVEILLANCE AND DATA SECURITY"

On August 22, 2022, the Federal Trade Commission published an advance notice of proposed rulemaking (ANPR) on "commercial surveillance and data security." The ANPR—advanced on a 3-2 vote of the FTC commissioners—solicits public comments on several different domains. General solicitations include the extent that consumers are harmed by commercial surveillance practices or lax security (especially children and teenagers), and how to appropriately balance costs and benefits. In addition to these, the FTC ANPR seeks specific comments on how, if at all, they should regulate commercial surveillance and data security. The FTC signaled interest in specific regulations related to (1) data security, (2) collection, use, retention, and transfer of consumer data, (3) automated decision-making systems (e.g., Artificial Intelligence), (4) discrimination based on protected categories, (5) notice, transparency, and disclosure, and (6) remedies.

In their solicitation for information concerning remedies, the FTC specifically expressed interest in profit disgorgement as a potential remedy for violations. Profit disgorgement refers to the

authority of regulators to take profits accruing from unlawful activity as a penalty for violating the law. Importantly, it is considered a comparatively severe penalty to contemporary enforcement approaches. [25,178]

C) OVERVIEW OF DIFFERENT APPROACHES TAKEN BY OTHER FEDERAL BILLS

As of May 2022, IAPP identified over 50 federal privacy bills introduced during the 117th Congress (not including the ADPPA).[4] Many of these bills share similar features. Many of these bills either outline specific consumer rights (notice and consent, data correction, data deletion, etc.), or impose specific obligations on businesses (data minimization, business practice disclosure, security, heightened rules for sensitive data, reporting requirements, risk assessments, etc.). Several federal bills limit their application to only large entities, but the definition of a large entity can vary considerably bill to bill (e.g., business with data on 50 thousand users annually versus businesses with data on 50 million users monthly). A few bills would specifically prohibit certain data practices, such as manipulating or misleading consumers, targeted advertising, or practices that promote compulsive usage. Several bills address specific or novel issues, including artificial intelligence and automated data processing, vaccination passports, protections for contract tracing data, and new rules for devices, services and apps that collect or use personal health data. One bill (S.3627) would create a central registry for consumer data deletion decisions and require data brokers without direct consumer relationships to register with the FTC. Another bill (H.R.2980) would establish an incentive program to promote cybersecurity. Some bills vest enforcement authority with the FTC. Other bills would create a new enforcement agency.

III. NEW PRIVACY AND SECURITY RISKS

A. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

Artificial intelligence machine learning tools present new benefits and risks. As a rapidly evolving technology, enacting laws that effectively mitigate risks while enabling socially beneficial technology applications is challenging.[11] (See Section V.C). Consequently, these new tools have evolved in a largely unregulated space.[10,11] This regulatory lacuna has created significant alarm due to the growing reliance on these tools across sectors.[12–14]

Real and potential risks to artificial intelligence and machine learning tools are varied and substantial. Economist Daron Acemoglu describes several social, economic, and political harms of artificial intelligence, including harms to (1) competition, (2) consumer privacy, (3) consumer choice, (4) excessive work automation, (5) increased inequality, (6) wage suppression, and (7) worsening political discourse.[18] Others have cited artificial intelligence's role in worsening racism, structural discrimination, and increasing inquities.[12–17] Given that these harms intersect multiple structural and social determinants of health,[19,20] it is reasonable to extrapolate that artificial intelligence applications could have substantial adverse health impacts as well. Importantly, as Acemoglu notes, these harms are likely not inherent to artificial intelligence, but they are derivative of the current underregulated uses of the technology.[18]

The capacity of artificial intelligence to enable powerful inferences from existing data is one reason why it is potentially transformative for privacy risk assessments. For example, a database might contain information on consumer behavior or purchase history. However, artificial intelligence might be able to infer or predict health status, loan repayment favorability, labor productivity, or predisposition to undesirable or illegal behaviors among endless other characteristics, qualities, and dimensions. These inferences extend the predictive power—and importantly the risks—of a dataset beyond the content scope of its constituent data elements.[10]

For these reasons, group harms are amplified in big data contexts. Group harms are those harms that adversely affect the collective interests of individuals sharing common characteristics.[179] In many artificial intelligence applications, the inferential or predictive processes that are developed are subsequently used to make decisions when relevant criteria are present. In short, algorithms define new groups that will either receive a benefit or harm from algorithm-based decisions.

Of course, the legal protections for a group will vary depending on its characteristics.[21] Wachter notes that different groups are protected differently—or not at all—by state and federal laws. For example, racial groups have protections under various U.S. anti-discrimination. Other groups identified by artificial intelligence processes might have substantial predictive

importance but are not legally protected groups (e.g., "dog owners").[180] Moreover, other groups derived through artificial intelligence might be incomprehensible to humans (e.g., users with specific mouse movement patterns).[21] Critically, data controllers might not be fully aware that the artificial intelligence tools that they deployed are harmful or discriminatory to groups or individuals.

B. INCREASING CONCERN OF LAW ENFORCEMENT USE OF HEALTH, HEALTH-ADJACENT, AND COMMERCIAL DATA

Many U.S. privacy laws have broad exemptions that permit law enforcement uses of protected data. Typically, a disclosure to a law enforcement agency under these exemptions will remove the data from the scope of the privacy law. Notably, this contrasts with the GDPR approach where some legal requirements will follow the data that is disclosed to law enforcement.[25]

There have been multiple high-profile stories that have raised alarms about the scope of law enforcement use of data. In 2018, law enforcement caught the notorious Golden State Killer by creating a fake profile on a commercial genetic database using samples from a rape kit.[22] Law enforcement was then able to identify the distant relatives of the suspect using the genetic results, which was sufficient to identify and arrest the suspect.[22] Notably, the suspect did not willingly contribute DNA to the commercial database, but was put at risk by the participation of a relative.[22,181] From a privacy perspective, it is important to expressly note that the individual consent protections relied upon by commercial DNA companies are insufficient to protect against the risks faced by distant relatives who share strands of DNA with the consenting individual.

While these methods enabled the conviction of long cold case, a more recent example highlights the risk that these practices pose to victims. For example, a woman is suing the city of San Francisco after officers allegedly submitted her rape-kit DNA to law enforcement database that revealed her as a suspect of a property crime that occurred years before.[182] This case raises concerns that these practices could discourage sexual assault survivors to seek assistance after their assault.

Similar concerns were raised following the Supreme Court decision in *Dobbs v. Jackson. Dobbs* overturned the decision in *Roe v. Wade,* which recognized a federal constitutional right to abortion.[23] Since *Dobbs*—and the activation in state trigger laws banning or criminalizing abortion—there is increasing concern that data indicating that a woman is planning on seeking an abortion or has received a now illegal abortion will be used for law enforcement purposes.[183] The HHS Office for Civil Rights released guidance on post-*Dobbs* disclosures to law enforcement under HIPAA that mostly just clarified that law enforcement disclosures are permissive not mandatory.[184] Notably, however, law enforcement do not need HIPAA-protected health information to prosecute suspects for receiving or providing health care that is now illegal. For example, police in Nebraska arrested a woman after discovering private Facebook messages that suggested that she was helping her daughter seek an abortion.[183] Private communication, social media posts, mobile health apps, and geolocation data can all be used to infer health status and can be potentially incriminating for women seeking abortions.[183]

In response to these new risks from clinical information, Professors Kayte Spector-Bagdady and Michelle M. Mello suggest that clinicians consider the medicolegal risks of documenting information in medical records and should ask themselves, "[w]hat information needs to be in the medical record to assure safe, good-quality care, buttress our claim for reimbursement, or comply with clear legal directives?"[185] They recommend that health care providers should be consulted to assert physician-patient privilege and consider whether law enforcement requests are mandatory or merely discretionary.[185] Ultimately, they argue, that broader privacy laws are needed to provide greater protections for those seeking care.[185]

Outside of health data, there are also broader concerns about law enforcement leveraging "surveillance capitalism" tools and services to enhance police surveillance and law enforcement capabilities. For example, the Associated Press recently reported that police agencies across the country have been using a cellphone tracking tool called Fog Reveal.[24,186] The tool allows police to search for "patterns of life" information derived from "hundreds of billions of records from 250 million mobile devices," offering "mass surveillance on a budget."[24] Similarly, several U.S. Senators raised alarm that U.S. Customs and Border Patrol has constructed a database of data

collected from thousands of Americans' phones and "permits thousands of employees to search the database 'for any reason.'"[187]

IV. PROMISING POLICIES, PRACTICES, AND TECHNOLOGIES

A. PREDOMINANT APPROACHES TO PRIVACY AND DATA PROTECTION

Many existing and proposed privacy frameworks align with one of four primary approaches. The first is a consumer protection model. This is the predominant approach in U.S. privacy law. Under this model, individual consumers are empowered with rights pertaining to the data about them. These rights often include the right to consent to data collection and use, but might also include rights of access, portability, correction, and deletion. Some consumer protection models create an individual right of action to remedy (and perhaps deter) privacy violations. However, a private right of action is often a point of contention in legislative debates on new privacy frameworks.

The second approach is a data protection approach to privacy. The European Union GDPR is the most recognized example of this approach. Under a data protection model, the rules governing data are grounded on principles concerning data collection, use, and disclosure rather than specific consumer rights. For example, the GDPR principles of data minimization and purpose limitation provide general rules for limited data collection and use.[188] These principles follow the data in a data protection framework. This ensures that protections are not dependent on consumers' omniscient diligence as data are shared and reshared. However, data protection approaches are sometimes criticized for being too vague and relying on general prudential principles rather than substantive standards.[25] As another example, UDPA includes some data protection provisions by including enumerated "prohibited" data practices. In contrast to a consumer protection approach, a regulated data controller would not be able to seek an individual's consent to conduct a prohibited data practice.

A third approach to data privacy incorporates ideas from antitrust by focusing oversight on entities of sufficient size. Many state and federal privacy proposals limit their application to entities that meet certain thresholds, including but not limited to (1) having data on X number

of individuals in a given period, (2) having Y dollars in total annual revenues, (3) deriving Z percent of annual revenues from selling personal data, or (4) some combination of X,Y, and Z. Cohen argues that for privacy rules that target dominant actors to have a meaningful effect on surveillance-based business practices they would need to disrupt corporate ownership, control structures, and licensed data flows.[25]

A fourth approach is the information fiduciary approach to data protection. First articulated by Professor Jack Balkin, in this approach data controllers have legal duties of confidentiality, care, and loyalty.[189–191] Implicit in these duties is an emphasis on good data stewardship and data governance practices as principal protective measures. For Balkin, this approach is preferable to the consumer protection approach because of the asymmetry of information between data controllers/processors and data subjects, who must trust that data controllers and processors will not betray or manipulate them.[190] This approach expressly recognizes the difficulties that individuals have in exercising their preferred privacy preferences given the complexity of issues and processes combined with the sophistication and opacity of large corporate data controllers and processors. The fiduciary duties of confidentiality, care, and loyalty must "run with the data," Balkin argues, to ensure that companies who do not directly interact with data subjects nonetheless are obliged to act with consideration of their well-being. In the context of massive data controllers and processors, Balkin argues that the fiduciary duties should be applied with the consideration of the broader population. Professors Lina Khan and David Pozen provide several critiques of this approach. Among these, they argue that in corporate contexts it would be difficult to manage the dual fiduciary duties of shareholders and data subjects, to which Balkin expressly admits that this approach will require sacrificing shareholder interests in favor of individual privacy interests.[190,192]

B. DIFFERENT ENFORCEMENT APPROACHES

There are a variety of enforcement alternatives options for privacy and data protection laws. Each alternative can be consequential for the effectiveness of a given regulatory framework.[25] Some enforcement choices come with preexisting jurisdictional limitations that effect the impact of the law. For example, delegating enforcement authority to a preexisting agency

would necessarily limit enforcement to the preexisting statutory authority of that agency without additional grants of authority. For example, some of the bills introduced in the 116th Congress delegated enforcement authority to the FTC without expanding their jurisdiction over common carrier functions of some information businesses leaving a regulatory gap and potential jurisdictional conflicts with other agencies (e.g., the Federal Communications Commission).[25]

Enforcement strategies have traditionally focused on two approaches: agency enforcement and enforcement through an individual right of action. For bills that rely on agency enforcement, some delegate enforcement authority to a preexisting agency, and others create a new agency or office responsible for enforcement. Either agency-based enforcement approach is dependent on funding. Only some bills create a fund that permits recovered enforcement penalties to fund future enforcement actions.

Other bills grant individuals a right of action to sue for privacy violations. Individual rights of action are controversial. From the regulated entities' perspective, an individual right of action opens a door to potentially endless vexatious litigation. Some privacy scholars have also questioned its effectiveness as both an enforcement mechanism and a deterrent. For example, Cohen argues that both public and private enforcement litigation cannot effectively discipline data practices that are widely distributed and produce group harms at scale.

Several alternatives to these two traditional enforcement approaches have been proposed, some of which have manifested in proposed privacy legislation. One approach is to deputize intermediaries to enforce standards and discipline within information ecosystems.[11,25,193] This approach has the potential to scale enforcement and oversight by conferring duties, traditionally associated with regulators, to private firms.[193]

Another approach would modify the standards and associated penalties to increase with the scale of the data activity or the size of the regulated entity. Professor Paul Ohm argues that there is an orders of magnitude problem in regulating large entities.[194] He argues that the scale of some firms or activities increases harm in a non-linear manner. For example, he argues that

human misery scales non-linearly, such that the harms associated with legal violations may be minimal at small scale (e.g., 10 victims in 10,000 users), but proportionally similar harms might be orders of magnitude more significant at larger scales (e.g., 1,000,000 victims in 1,000,000,000 users).[194] Accordingly, he argues that standards and associated penalties should increase with the scale of the activity or the size and sophistication of the regulated entity.

In her criticism of contemporary U.S. privacy proposals, Professor Julie Cohen argues that two underutilized penalties are profit disgorgement and personal liability for corporate executives.[25] Disgorgement is being increasingly explored as an enforcement tool (see discussion of the FTC ANPR in Section II.B.2.b above). It is a comparatively severe penalty which shifts the cost-benefit analysis of data controllers and processors by permitting the enforcement agency to claim all profits derived from the illegal activity as part of the remedy. Personal civil or criminal liability presents another comparatively severe penalty to decisionmakers within the corporate structure of data controllers and processors. To be effective, a personal liability approach might need to adapt veil-piercing mechanisms from corporate law.[25]

V. POTENTIAL PROBLEMS IN GOVERNANCE OF HEALTH INFORMATION

A. PROBLEMS AND GAPS IN EXISTING LEGAL PROTECTIONS

The U.S. privacy framework is often derided as a patchwork of laws.[26–31] This patchwork is both overly complex and under protective. These criticisms have led to calls for federal privacy legislation from both industry and privacy advocates alike.[30,31,34–38,195]

The U.S. legal privacy framework is under protective when its sector-by-sector and jurisdiction-by-jurisdiction approach leaves personal information un(der)-regulated. In particular, the absence of legal protections for data in commercial settings has long been criticized by privacy advocates. While the FTC has authority to take enforcement actions for some privacy violations (e.g., those that are "unfair" or "deceptive" practices), their authority has been criticized as "toothless."[32,33] Solove and Hartzog have described how FTC has used its enforcement actions

to create a "new common law of privacy" by establishing privacy standards by treating enforcement settlements as *de facto* precedents.[31]

Nevertheless, the sectoral approach leads to uneven protections that can be confusing to consumers.[34] For example, consider a patient's electronic health record. That health record is maintained by a vendor that is a business associate of a HIPAA covered entity; therefore, the patient's electronic health record is protected by the robust privacy and security provisions of the HIPAA regulations. However, if the patient requests that the covered entity export their electronic health records into a *personal* health record application controlled by the patient but operated by a private, non-covered entity business, then the robust HIPAA protections now no longer protect the same data.[196] Yet, consumers might still incorrectly assume that the well-known health privacy law still applies.[197] The same regulatory gap exists for health data collected and processed by commercial entities, like fitness tracker apps, menstrual trackers, or social media communities relating to health conditions. Parasidis, Pike, and McGraw cited the regulatory inconsistency of health data in their 2019 call for a new Belmont Report to govern processing of health data in all contexts.[34]

The U.S. privacy framework is also overly complex. Jurisdictions—responding to the regulatory gaps describe above—have begun enacting their own privacy laws. However, these jurisdictional approaches are not always consistent. This jurisdiction-by-jurisdiction approach complicates the existing sector-by-sector approach of many privacy laws.[26,29,30,35–37,195,198–200] All this variability makes compliance exceptionally difficult, especially for large data controllers and processors. This is one reason why industry has embraced calls for a national comprehensive privacy law; they hope such a law would simplify compliance even if it imposed stringent requirements.[35–39]

Notably, while the U.S. privacy framework is under-protective in some respects, it might be *over*protective in other aspects. For example, a privacy law might be considered overprotective when it restricts popular and socially beneficial data uses.[28] For example, a 2020 national survey of U.S. adults measured privacy preferences relating to the secondary use of identifiable personal data.[40] The survey measured respondents' comfort with 72 different data use

scenarios with variations on the data processor (i.e., government, business, non-profit, and university), data type (i.e., health data, education data, government program data, and commercial data), and data use purpose (i.e., research, profit-driven, law enforcement, marketing, and promoting population health). Ironically, the survey results suggest that the U.S. public is most comfortable with a university using identifiable education records for promoting population health—a use that is restricted by FERPA—and least comfortable with businesses using commercial data for profit—a use that is subject to relatively loose oversight.[40] This represents one example where privacy protections might impede a data use or practice that is both socially beneficial and popular.

B. SPECIFIC ISSUES IN PRIVACY POLICY DEBATES

1. DEFINING AND REGULATING SENSITIVE DATA

Different types of data can be associated with different types and magnitudes of harm. For example, data describing patients' HIV status might carry increased risk of stigmatization harms.[201–203] For this reason, some privacy laws provide heightened privacy protections for sensitive information (See Section II).

However, additional privacy protections may come at an unanticipated cost. For example, there are good reasons to have heightened protections for data containing information on race and ethnicity. These data can facilitate invidious and insidious structural discrimination and racism.[12–15] This is a magnified risk where automated data processing algorithms identify existing disparities and inequities as good predictive criteria and reinforce them through new automated decision-making processes. However, over-protecting race and ethnicity data can have an unanticipated effect of hiding existing disparities and inequities through inadequate reporting for vulnerable groups (see discussion of data genocide in Section V.E.1 below).[204,205] In many cases, communities have demanded a right to be counted, arguing that knowledge of harm empowers communities to advocate for remedies (See Section V.F.2).[205,206]

2. PREEMPTION OF STATE LAWS

Preemption is a critical issue in current federal privacy debates.[8,175] Industry representatives currently push for aggressive preemption because they stand to benefit from a simplified regulatory regime, regardless of whether the new protections are more stringent than the preempted laws.[35,36,38,39] Without preemptive provisions, a new federal law only complicates already complicated compliance systems. In contrast, privacy advocates in some states have fought long and hard political battles for certain privacy protections, and they do not want to lose those protections to a preemptive federal law. For example, Speaker Pelosi recently came out against the bi-partisan ADPPA because it preempted some of the substantive protections in California's comprehensive privacy law.[8]

The ADPPA—described as a consensus bill—is a useful example of compromise in preemption.[207] The July 22, 2022 version of the ADPPA generally prohibits all comprehensive state privacy laws, but expressly preserves enforcement actions by the California Privacy Protection Agency and the CPRA's individual civil action provisions.[56,177] The ADPPA also preserves various non-comprehensive state privacy laws, including law pertaining to the privacy of health information and HIV status.[177] These extensive and detailed exceptions suggest that preemption is a tricky issue requiring careful consideration and compromise.

3. TREATMENT OF EXISTING FEDERAL LAWS

In current national comprehensive privacy debates, there are open questions about what to do with existing federal privacy laws. On one hand, a comprehensive privacy law could replace existing federal laws—eliminating the currently derided "patchwork"—and provide a single set of standards across sectors. This would be a similar approach to the European GDPR. However, this would be a substantively more difficult political and legislative task, and achieving consensus may require a different approach. As noted by Stacey Gray, Director of Legislative Research and Analysis at the Future of Privacy Forum, "I have not spoken to anyone at the state or federal level that is interested in reopening and renegotiating HIPAA."[175] Consequently, it is likely that any future federal privacy efforts will focus on filling holes within the existing patchwork of laws rather than replacing the patchwork.

If existing federal laws are left in place by future federal comprehensive privacy legislation, there at least four approaches to accommodate those laws. First, a new comprehensive privacy law could be carefully crafted to avoid overlapping protections; however, this approach is usually not practical due to the broad definitions of protected data and covered entities typical of comprehensive bills. Second, a new comprehensive privacy law might exempt *entities* covered by other privacy laws; however, this approach can be problematic if certain entities are subject to some parts of a federal privacy law, but engage in other underregulated activities.[175] For example, Amazon is a HIPAA hybrid entity, so it could be exempted from coverage of a law that exempts entities subject to HIPAA.[175] Third, the new comprehensive law could exempt *data* that are subject to protections under another federal privacy law. According to Stacy Gray of the Future of Privacy Forum, exempting already covered data is preferable to exempting already covered entities. Fourth, a new comprehensive privacy law, can deem entities compliant with the new law if they are compliant with an existing law. This has the effect of "two-ply" protection whereby an entity is subject to penalties under both laws but only needs to comply with one.[28] Both the ADPPA and the UPDPA use this two-ply approach to existing federal laws.[177,208]

4. INCLUSION OF AN INDIVIDUAL RIGHT OF ACTION AS AN ENFORCEMENT APPROACH

Another major point of contention in national privacy debates is the inclusion of an individual right of action against data controllers and processors.[175] Including private rights of action in legislation is often a key priority for privacy advocates, but it is vigorously opposed by many in industry. Notably, some privacy scholars are critical of private rights of action as a principal enforcement mechanism.[25] For example, although Cohen acknowledges the value and important role of enforcement through litigation, she notes that privacy litigation has serious limitations as a primary enforcement mechanism, saying "because enforcement litigation is predominantly atomistic in its identification and valuation of harms, it cannot effectively discipline networked phenomena that produce widely distributed, collective harms manifesting at scale."[25]

5. IMPLICATIONS OF FUTURE PRIVACY LEGISLATION FOR HEALTH CARE AND PUBLIC HEALTH INFORMATICS

As health care and public health informaticists increasingly focus on social, economic, and structural determinants of health, they are increasingly exploring the use and combination of non-traditional and cross-sectoral data.[19,200,209–213] Critically, however, public health exceptions are relatively rare in privacy laws.[26,28,200] The absence of these public health exceptions reinforces the legal and policy barriers for public health data sharing.[214–216] Including public health data use exceptions in comprehensive privacy legislation might be required to enable anticipated health benefits of big data and health information technology.[28,217]

C. ARTIFICIAL INTELLIGENCE, MACHINE LEARNING, AND BLACK BOX DATA PROCESSING

Artificial intelligence and machine learning refer to the algorithms that assist processes and decision-making by optimizing performance using a predetermined set of outcome criteria. For example, an advertiser might want to identify customers most likely to purchase a product. A data processor might use artificial intelligence to identify a consumer profile that has a high probability of purchasing the product using a large dataset of consumer attributes and purchasing history. The algorithm would sift through potentially millions of consumer attributes and build a profile that maximizes the association of attributes with purchasing the product (or similar products). The attributes the algorithm ultimately identifies could be incomprehensible to the human developer (e.g., computer cursor movement patterns), yet have tremendous predictive power.[21] In this example, the developer defines the desired outcome criteria, and the machine learning process uses the available data to get there.

Artificial intelligence and machine learning are often referred to as black box processes because they are inherently opaque. The ultimate decision-making criteria are determined by automated algorithmic processes, and it might not be immediately clear whether the artificial intelligence-driven decisions are equitable or what groups are affected. This section addresses some of the opportunities and challenges posed by these technologies in the domains of privacy and confidentiality regulations.

Similar processes can be used in health contexts. Artificial intelligence can identify patient profiles that—based on data attributes in patient medical history, genomics, present biomarkers, and gut biome—determine which treatment option has the greatest likelihood of success (i.e., precision medicine). Similarly, artificial intelligence algorithms can identify patient cohorts suitable for pragmatic clinical trials, inform clinical decision support tools embedded in electronic health records, and identify relevant scientific literature pertaining to a given patient's condition (i.e., dimensions of a learning health system).[218–224]

However, artificial intelligence can also exacerbate inequities. For example, a health system might employ artificial intelligence tools to help evaluate locations for a new clinic location. If the algorithm maximizes profitability as an outcome criterion (without constraints or countervailing criteria) the algorithm might identify locations in affluent areas, where residents tend to have higher-reimbursing private insurance plans. At scale, this might mean that socially and economically underserved communities are continually overlooked, ensuring greater disparities and inequities for these populations.

1. RAPID TECHNOLOGICAL ADVANCEMENTS MAKE A MOVING REGULATORY TARGET

Across domains, technological innovation tends to far outpace the ability of regulators to manage new and emerging social issues and risks.[225] Artificial intelligence, machine learning, and big data analytics generally are not immune from this phenomenon. For example, in Solove's criticism of the UPDPA, he argues that it was "obsolete on arrival."[158] The part of the difficulty in regulation stems from definitional challenges. Developers, scientists, and regulators have all struggled to define what constitutes activities like "big data" or "artificial intelligence."

Additionally, the scope of potential applications is virtually unknowable, further challenging regulators' ability to adequately balance risks and benefits within a static regulatory framework.[226,227] Artificial intelligence and machine learning algorithms have enormous potential to identify and solve new challenges as well as improve efficiencies within health systems. For example, artificial intelligence processes are likely to serve as the algorithmic backbone for learning health systems, precision health care, and precision public health.[209–

[211,218,221,228] However, there are concerns that artificial intelligence can contribute to individual and collective harms. Regulators have the challenge of creating rules that balance mitigation of existing and potential harms, while enabling existing and potential benefits. This balance is a substantial challenge for a rapidly evolving technology like artificial intelligence.[11]

Risks of unintended consequences from well-meaning regulatory approaches compound this challenge. For example, civil rights groups have pushed for greater civil rights protections in federal privacy legislation.[229] As an example, race and ethnicity data are classified as sensitive data in a recent draft of the ADPPA.[171] There are legitimate reasons to protect these data, as race and ethnicity data can facilitate structural inequities. However, there is a risk that strict protections could inhibit the use of race and ethnicity data to discover, understand, or address existing structural inequities.[10] In other words, what is not counted, does not count.[206] Given that many artificial intelligence applications are still nascent, many potential risks and benefits are still unknown. Consequently, existing (or future) privacy frameworks could unintentionally exacerbate a risk or inhibit a benefit of artificial intelligence.

D. PROTECTING DATA WHILE ENABLING ETHICAL USES

Legal privacy and data protections sometimes come into tension with collective interests when protections for individual rights inhibit socially beneficial activities.[28,230,231] For example, Professors Jane Bambauer and Brian Ray noted that technological efforts to track COVID-19 infections were hindered by "state and federal governments (as well as influential private firms) . . . prioritizing a fetishized notion of individual privacy over collective public health."[232] They asserted that singular focus on consumer rights (i.e., individual privacy, opt-in requirements) led to critically flawed platforms, "destined to be useless."[232] In contrast, the South Korean government integrated multiple data sources—including geolocation, transaction, closed-circuit recording, facial recognition—to supplement traditional contact tracing efforts.[232] Professor Alan Rozenshtein asserts that mandatory "digital disease surveillance" is valuable but stops short of an endorsement, arguing that "dangers to privacy,

liberty, and equality" are ever present, and "there is no guarantee that such surveillance will be well designed."[233]

Regardless, many ethicists have noted that in some situations individual interests must give way for collective well-being.[216,234–241] Ensuring that the tradeoff between individual and collective interests is ethically sound can be challenging. One approach is to seek a "social license" from relevant communities or groups. Social license refers to the informal permission given by a community to a public or private entity to engage in a specific activity.[242] In big data contexts, a social license provides legitimacy to collect, use, or share data within relevant communities as well as help to establish credibility and trust between communities and data processors.[243] Social license is often developed through careful and appropriate community consultation and engagement. [244,245] For example, the World Health Organization cites community consultation and involvement in decision-making as one way to support ethical surveillance activities.[234]

It is important, however, to acknowledge that many of the scandals and abuses that impelled the development of the canons of bioethics were conducted by physicians and researchers under the false aegis of social benefit.[246–250] Consequently, there are good reasons to be cautious about legal approaches that liberally permit a subordination of individual rights without appropriate conditions and guardrails.[234,251]

1. RECOMMENDATIONS FOR PANDEMIC SURVEILLANCE

Bambauer and Ray argue that a pandemic-driven data surveillance system should have four essential elements.[232] First, they argue that a pandemic surveillance system should be a "springing data repository" that is automatically authorized and activated upon a pandemic declaration. This "springing data repository" would include a data collection program that incorporates the functions and flexibilities of commercial technologies. Second, they argue that the pandemic surveillance system should incorporate robust access limitations. These limitations should be restricted to permit only public health activities and should expressly restrict redisclosure of data and specifically prohibit law enforcement use of data. Third, Bambauer and Ray argue that the system should be transparent by design to enable open

public scrutiny, including available source code, access logs, and recorded non-routine uses of the system. Finally, they argue that a pandemic surveillance system should have an automatic sunset provision that terminates the system when the need for it no longer exists. [232]

2. DATA SHARING BETWEEN FEDERAL, TRIBAL, STATE, AND LOCAL PUBLIC HEALTH PARTNERS DURING THE PANDEMIC

U.S. public health responsibilities are divided between local, state, tribal, and federal partners. Each of these partners have legitimate and often overlapping authority and governmental interests. Perhaps as result, data sharing between these partners encountered substantial friction during COVID-19 response, straining inter-governmental and inter-agency relationships.[204,252,253]

In the case of syndromic surveillance, the data use agreements (DUAs) between the CDC and state/local partners impeded the response to COVID-19 by restricting federal access to HHS region-level syndromic surveillance data.[251,252,254,255] Under these restrictions, for example, federal National Syndromic Surveillance Program (NSSP) personnel – cannot distinguish, whether an observed increase of a syndrome in HHS Region 10 is (1) an isolated event in Washington, (2) unrelated, but similar, events in Washington and Alaska, or (3) related events in Washington and Oregon.[251,252,255] These access restrictions are despite maintaining these data for all state and local NSSP participants. In an apparent exercise of emergency authority, the White House COVID-19 Task Force obtained access to all COVID-19 NSSP data in early 2020.[256] Although the federal government was able to bypass these policy barriers, the decision left some state and local epidemiologists feeling that the agreed upon DUA policies were "thrown out the window."[252,253]

Inter-governmental data sharing issues were also experienced by tribal public health partners. In a 2021 report, the Urban Indian Health Institute equated deficient data collection and data sharing with tribal public health organizations and Tribal Epidemiology Centers with data genocide of American Indians and Alaskan Native (AI/AN) populations.[175,204] The report argues that inequitable systems that suppress, misclassify, or fail to collect certain minority population data "have inhibited representation of AI/AN in public health surveillance systems resulting in

deficit-based data and invisibility through data erasure."[204] By not counting (or reporting) these communities, the report argues that the disproportionate and inequitable impact of COVID-19 on these communities was hidden from public view.[204] The report makes several recommendations for improving public health surveillance, including (1) mandating and enforcing the collection of race/ethnicity data, (2) providing additional resources for public health surveillance, (3) standardizing race/ethnicity data collection, (4) avoiding homogenizing categories like "other" or "multiracial," and (5) disaggregating "multiracial" categories.[204]

Notably, some of the most potent public health data sharing barriers are relationships and trust between partners, in addition to legal and policy barriers.[257] Critically, the relationships and trust between federal, tribal, state, and local partners was shaken during the COVID-19 response.[175,204,252] One key informant to a 2021 study by the Council of State and Territorial Epidemiologists noted:

> "*There's been such a lack of trust that has been reinforced during [the COVID-19] response. I think it's actually going to be harder rather than easier [to permit greater federal access to state or local data]. I say that anyway because I think the NSSP program itself, in its current form, and I think it's probably important that this gets documented, has been an amazing steward of the data, but the system around it has become less trustworthy and I think the system around it and the system, the way that the response has worked with the states, is now going to impact the program's ability to do its best work. So, in today's world, CDC has become less and less willing to really talk to states in pre-decisional ways and help states understand this data is driving this decision, and there's been a much larger tendency for CDC to make decisions and then just inform states about it in this response. And so, I think pre-COVID, it actually would have been easier rather than harder to implement some of these changes right now, in a way that the states felt good about.*"[252]

As a result of these trust issues, any new policies that facilitate greater public health data sharing among public health partners might require substantial guardrails to ensure that any shared data is used only for appropriate public health purposes.[251–253]

E. SUFFICIENCY OF DE-IDENTIFICATION AS A PROTECTIVE MEASURE

There are two principal reasons to de-identify data. First, a data controller might de-identify a dataset to comply with a legal standard. Once legally de-identified, the legal protections applicable to the data might be reduced, permitting the data controller to use the de-identified data in ways that might not otherwise be permitted with more identifiable data. Second, data might be de-identified as an ethical precaution. In this case, the data are de-identified to reduce the potential risks to the data subjects, but the de-identification might not be legally required for the desired purpose. Neither of these examples describe mathematically de-identified data.[258]

Legal de-identification standards demarcate when less stringent legal protections apply to the data (if any). These reduced protections are justified by the theoretically reduced risks of identification to data subjects. However, there is an ongoing "arms race" between technical methods of de-identification and re-identification.[175] Increasingly sophisticated methods of re-identification now call into question whether dated legal de-identification standards sufficiently protect data subjects to justify reduced legal restrictions. The HHS Office for Civil rights last provided guidance for de-identification in 2012.[259] Since then there have been calls and recommendations for updated operational guidance on de-identification methods.[175,260] For example, nearly every panelist on the NCVHS July 2022 full committee meeting cited ongoing issues with de-identification. Importantly, NCVHS provided 12 recommendations to HHS to improve de-identification practices in 2017; however, no apparent actions based on these recommendations were taken.

Notably, some ethicists have begun to question the focus on de-identification as a data protection. For example, Megan Doerr of Sage Bionetworks has argued for the "need to dispense with the theater of anonymity" and acknowledge that some data are inherently identifying (e.g., location data).[261] In these contexts, she argues, de-identification is the wrong approach to mitigate harms. In contrast, building or establishing a "social license" for data

collection and use might be more appropriate and protective than de-identification, which is vulnerable to continually evolving re-identification methods.[261]

1. GROUP HARMS FROM DE-IDENTIFICATION

The assumption that de-identification reduces risks by rendering a data subject more difficult to identify can be questioned in big data contexts.[262] For example, often the objective in big data applications is to gain insights about groups of people with similar characteristics.[262] While some of these group insights can be helpful, others can contribute harm to groups and the individuals within them. De-identification cannot eliminate these group risks and might aggravate them. De-identification choices can affect how data are interpreted by affecting how data can be aggregated and summarized. For example, truncating ZIP codes restricts geographic units of analysis into certain groups. Similarly, aggregating data by racial groups could facilitate erroneous stereotypes. Alternatively, suppressing racial groups due to a "low cell size" can systematically suppress critical information about that group.[204] While de-identification might protect the individual data subjects, it affects the analysis—and the associated risks—to the groups that the data subjects belong to.[262]

F. INCREASING SKEPTICISM OF CONSENT AS A SUFFICIENT PROTECTIVE MEASURE

Historically, U.S. privacy laws have focused on mitigating individual harms experienced by data subjects.[10,263] This focus reflects the influence of the foundational canons of bioethics—including the Declaration of Helsinki[250] and the Belmont Report.[248] These foundational documents established the central tenets of bioethics and emphasized the principle of respect for persons.[28] In practice, informed consent became the primary tool to support individual autonomy and respect for persons. In the context of established certain relationships—such as researcher-patient or physician-patient relationships—informed consent requirements can be powerful protective measures.

However, contemporary data protection laws' reliance on consent (i.e., consumer protection models) are coming under increasing scrutiny.[10,25,264,265] For example, Cohen argues "[t]he

continuing optimism about consent-based approaches to privacy governance is mystifying, because the deficiencies of such approaches are well known."[25] In the recent ANPR, the FTC has acknowledged some of these deficiencies noting that "the permissions that consumers give may not always be meaningful or informed," and FTC has sought information on what opacity "mechanisms" are used to obfuscate disclosures concerning data practices.[266] For example, the FTC and some states have grown increasingly concerned with "dark patterns" or user interfaces designed or manipulated to subvert or impair user autonomy, decision-making or choice.[73,266] Recognizing these deficiencies, Solove notes "[m]odern laws have been moving away from the notice-and-choice approach, and even those that adopt it at least make some attempt to reign it in or otherwise make it less noxious."[158] This section reviews some of the challenges and criticisms of the traditional "notice and consent" consumer protection model and describes a few recommendations for addressing these issues in the law.

Generally, consumers' attitudes reflect a preference for limiting the collection of their personal information and a skepticism of sharing of their information with third parties.[28,267–270] Certainly, privacy attitudes vary within populations and can be shaped by consumer experience.[271,272] However, mounting evidences suggests that notice and consent approaches might only provide illusory control. For example, a substantial body of evidence documents an incongruence between consumers' stated privacy attitudes and their privacy behaviors. Specifically, this "privacy paradox" is a phenomenon where individuals might have strong privacy concerns, yet often they will casually give personal information if requested even where the benefit is a *de minimis* benefit.[273–276]

However, the privacy self-management required under notice and consent privacy laws has both structural and substantive complexity challenges. For Solove, the observed privacy paradox reflects a structural problem rather than consumer inconsistency.[265] Solove argues that the time cost required to assess each privacy option presented to a consumer is massive.[265] Others argued that even well-crafted privacy notices and interfaces are unlikely to help consumers if consumers are faced with hundreds of privacy notices annually.[25,277,278]

Solove argues that the privacy self-management approach (i.e., notice and consent) "is being tasked with doing work beyond its capabilities."[265]

Other legal scholars have questioned whether lay consumers are able to fully comprehend the analytical complexity, and increasing sophisticated algorithms, of big data processes—as well as all associated implications—that are described in company privacy policies.[10] For example, a consumer might not fully appreciate the significant inferences that can be made from personal data that indicate that they play video games, own a dog, or click their mouse compulsively might affect the terms of a car loan that they receive.[21] Nonetheless, sophisticated artificial intelligence and machine learning algorithms might enable companies to use otherwise innocuous information to make powerful predictions that put consumers at risk of loss or harm.[21] According to Professor Alicia Solow-Niederman, "[m]achine learning analytics make it practically impossible for an individual to determine how data might or might not be significant or sensitive in a future setting."[10] Moreover, the protection from a notice-and-consent model often fails to account for how publicly available information may be combined with protected data using complex and opaque machine learning to profile persons who have not consented to being profiled.[28,279]

Even the most sophisticated consumers might be unable to fully weigh the risks and benefits needed for truly informed consent. While the notice and consent approach was developed to promote individual autonomy and mitigate individual harm, Solow-Niederman argues individual rights to opt into or out of data collection or subsequent uses won't help if there are flaws in the individual control model to begin with."[10]

1. AN INFORMED CONSENT BLIND SPOT: GROUP HARMS

Informed consent rights rest on the assumption that risks and benefits are best evaluated by the affected individuals. Accordingly, informed consent works best as a protective measure when the risks and benefits of a data activity are easily understood by data subjects. This permits data subjects to balance all factors and take personal values in consideration, ultimately deciding if the benefits outweigh the potential risks for the individual. However, the reliance on notice and consent protections inherent in the consumer protection model largely

overlooks the risks and harms experienced by the groups data subjects belong to.[10] Increasingly, big data analytics implicates risks and harms that accrue to groups. These types of risks are not adequately accounted for where notice and consent is the primary protective mechanism for individual privacy, including research contexts.[280] Megan Doerr of Sage Bionetworks has noted that for many types of data and processing, individuals are "never truly alone" and individual consent may be insufficient where an individual's data might provide insights for others.[261]

For example, an individual who consents to genetic research could face *de minimis* individual risk, but the research activity might develop insights about a group the individual belongs to that could result in substantial group harms. For example, the individual's genetic data can be collected with minimal risk, but the insights from the genetic data can have extensive effects on the individual's family, community, and culture.[281] Often these types of collective harms are undervalued by individuals.[25]

Moreover, the complexities of modern data analytics strain the capacity of even the most sophisticated individuals to fully understand implications of their "consent."[10] Methodological opacity and complexity impedes informed or meaningful consent.[10] For example, many Facebook users likely did not appreciate that the broad consent they provided enabled widespread emotional experimentation on vulnerable users.[282] For an individual to protect against group harms by withholding their consent, the individual must have awareness of the group(s) they belong to and have the capacity and willingness to weigh those group harms and benefits alongside their individual risks and benefits. The consumer protection approach to privacy "assumes that it's possible for a person, at the time that they are presented with a privacy policy, to assess the consequences that might flow from releasing personally identifiable data."[10] The consumer protection approach risks being under-protective when it does not account for how data might be used about consenting and non-consenting data subjects.[28]

Importantly, group harms can extend beyond the specific scope of the data being analyzed.[262] For example, a researcher investigating school performance reports only student performance

data aggregated at the school level to protect individual students. While reported data concern only specific schools, the neighborhoods around badly performing schools could experience decreasing property values and increasing community stigma. Critically, the harmed neighborhood residents were not the focus of the study, so they might not have had the opportunity to communicate their concerns with the researchers. Similarly, an individual who provides consent for a data activity could enable harms that accrue to external groups.[262]

Indeed, much of big data predictive analytics is focused on deriving insights from a sample to make predictions about a much larger group or population. In the notice and consent paradigm, the sample population might have been afforded the opportunity to decline participation in the development of the algorithm. However, a much larger group or population might become subject to the risks and benefits of the developed predictive algorithm or profile without necessarily providing consent. Professors Solon Barocas and Helen Nissenbaum describe this dynamic as the "tyranny of the minority."[283]

2. RIGHT TO CONSENT AND THE RIGHT TO BE COUNTED

Some ethicists have argued that another individual right often countervails a right to consent to data use: the right to be counted. For example, Professor Amy Fairchild has argued that individuals and the communities they belong to have a right to be counted.[206] She argues that information can empower individuals and communities to act. For example, assume an industry is harming a community through environmental contamination. The harm will likely continue if it remains unknown. However, once the harm is discovered (e.g., through epidemiological study), the discovery empowers the individuals within that community to act to seek new regulations, sanctions, penalties, or remedies in response to the harm (as what occurred in Love Canal, NY).[284]

Similarly, the act of counting informs important resource allocations. As a corollary, inequitable counting begets inequitable resource distributions.[262] Left unchecked, inequitable counting can contribute to "data genocide", whereby the undercounting of a particular group contributes to systemic exclusion of a group (and eventual extermination).[204] For example, the Urban Indian

Health Institute asserted that deficient reporting and sharing of COVID-19 surveillance data with tribal communities amounted to data genocide of AI/AN populations.[204]

3. THE INFORMATION FIDUCIARY MODEL TO DATA PRIVACY

The information fiduciary model is one emerging alternative to the "notice and choice" paradigm.[189,190,192,285,286] Professor Jack Balkin describes the model as a "movement to viewing privacy in relational terms of trust and trustworthiness."[190] According to Balkin, the fiduciary obligations are derived from "social relationships, and the power and vulnerability inherent in these relationships," regardless of whether those relationships are doctor-patient or teenager-Facebook.[190] Balkin contends that the information fiduciary approach is necessary to address the problems created by information capitalism, namely the vulnerability and dependence of consumers on large data controllers and processors.[190]

In the information fiduciary model, data controllers and processors of personal data have three fiduciary duties: care, confidentiality, and loyalty. Balkin argues that these duties should "run with the data," which might require a separate duty to "vet" data partners and downstream data processors.[190] In particular, the duty of loyalty requires that data controllers and processors act in the data subjects' interest and "means that digital companies may not manipulate end users or betray their trust."[190] However, the duty of loyalty extends beyond the individual to the broader public as Balkin describes it. He argues that "large platforms like Facebook, Google, and Amazon have so many end users that a requirement that they must act in the interests of their end users effectively requires them to act in the interests of the public as a whole."[190] Consequently, it is possible that the information fiduciary approach might be amenable to the group harm considerations discussed above.

4. CONSUMER PROTECTION VERSUS DATA PROTECTION

In contrast to the consumer-focused data privacy model used in most U.S. privacy laws, some have argued for adopting a more European data protection framework.[264] For example, Professors Chander, Kaminski, and McGeveran argue for the importance of data protections that "follow the data" regime like those in the GDPR.[264] For example, imposing duties of data

minimization and purpose limitation provide persistent restrictions for data controllers and processors to ensure that they do not expose consumers to excessive risks. Professors Chander, Kaminski, and McGeveran note that one of the important features of the GDPR data protection approach is that it establishes the "default in Europe . . . that personal information cannot be collected or processed unless there is a specific legal justification for doing so."[264]

5. POPULATION-BASED APPROACHES TO RESPECT FOR PERSONS

Informed consent is the primary tool used to support the respect for persons ethical principle in research and clinical contexts. However, in population-level activities other approaches to support respect for persons have been employed. For example, in public health surveillance, consent requirements can be problematic because non-participation of a relative few can bias results and frustrate collective benefits.[205,234,241,287–289] Consequently, public health ethicists take a different approach to support the "respect for persons" principle, and recommend involving communities in the decision-making process for population-level interventions.[234] This approach helps establish a social license for the activity as discussed above.[242,243,245] Similarly, many big data applications also must reckon with the unique ethical challenges associated with population-scale.[240] As an example, the public backlash to the Google and Ascension joint venture (i.e., Project Nightingale) could be attributed to a failure to establish a social license with patients and healthcare providers to engage in that data activity.[290,291]

G. OTHER ISSUES AND TOPICS FOR FUTURE CONSIDERATION AND EXPLORATION

- New harms and benefits from data linkage techniques
- Privacy-preserving technologies and techniques
- Legal obligations and protections that "run with the data" (e.g., duties of data minimization, purpose limitations, care) after permitted disclosures.
- The Common Rule's evolving definition of identifiable information given new techniques and methods of uniquely identifying data subjects.

VI. OPPORTUNITIES FOR TIMELY ADVICE FROM NCVHS TO THE HHS SECRETARY REGARDING CONSTRUCTIVE ACTIONS THAT HHS AND OTHER FEDERAL DEPARTMENTS MIGHT TAKE.

A. DE-IDENTIFICATION

De-identification remains a critically important issue in privacy. Nearly all panelists in the July 21, 2022 NCVHS meeting cited issues tied to deidentification.[175] Notably, NCVHS submitted 12 recommendations on de-identification to HHS in 2017. However, it is not clear that there has been subsequent action on these recommendations. Since then, the privacy and security landscape has continued to change and evolve, often dramatically, in response to technological developments and world events. Nevertheless, the NCVHS panelists clearly suggested that de-identification issues persist. In particular, existing operational and technical guidance on de-identification is increasingly out of date.

The 2017 NCVHS recommendations on de-identification remain highly relevant to contemporary issues. Moreover, changes since 2017 might warrant revisiting these recommendations because of changing priorities, environment, and the likely substantial distraction of the COVID-19 pandemic. In addition to the 2017 recommendations, NCVHS might consider exploring considerations of both individual and group harms related to methodological approaches in data aggregation and de-identification (e.g., see Section V.E.1).[175,204]

B. LIMITATIONS ON LAW ENFORCEMENT ACCESS TO HEALTH RECORDS.

Recent concerns about law enforcement access to and use of private information raise parallel questions about whether existing law enforcement disclosure exceptions in some privacy laws might enable inappropriate uses. Law enforcement disclosure exceptions in laws like HIPAA are often quite broad. However, there are notable exceptions; for instance, 42 C.F.R. Part 2 significantly curtails law enforcement access to substance abuse disorder treatment records, in part to encourage those that need help to seek needed services.

However, drawing the line between appropriate and inappropriate law enforcement uses of health data could be quite challenging. Consider a patient that seeks care for a gunshot wound

as compared to a pregnant patient who seeks abortion care for a non-viable fetus in a state that has banned abortion. Records for both these patients would likely facilitate law enforcement investigations of a potential crime. However, public concerns have been raised for the latter example and not the former. An NCVHS convening could help refine and identify nuance within this area. Some issues could be explored in more detail. These include,

- Narrowing the scope of the HIPAA law enforcement exception.
- Imposing data protection requirements on data disclosed for law enforcement purposes, such as principles of data minimization and purpose limitation (similar to the EU approach).
- Imposing higher legal standards and restrictions for generalized (as opposed to individualized) law enforcement data requests.

C. ALGORITHMIC PROTECTIONS

Increasingly, artificial intelligence and machine learning tools are reshaping the structures of health care delivery as well as broader social structures. Existing federal laws do not distinguish between these automated processes as compared to traditional manual data uses and practices. However, the risks associated with these automated processes are fundamentally different in scope and scale (See Sections III.A and III.E). A future NCVHS convening could explore the following issues:

- Feasibility of standards and requirements for conducting impact assessments—similar to some proposed and enacted state laws—that evaluate or predict the impact of algorithms in areas such as unlawful discrimination, inequitable impact, or group harms.
- Requirements or standards for increased transparency on the use of and purpose for automated data processing tools.
- Higher standards, duties, or penalties based on the size and sophistication of the data controller.

D. INPUT AND COLLABORATION ON THE HEALTH IMPLICATIONS OF THE PENDING FTC RULEMAKING

There are important health implications for the FTC ANPR on Commercial Surveillance and Data Security. (See Section II.B.2.b). The FTC has jurisdiction over many HIPAA covered entities, so future rules could create compliance confusion or have unintended impacts on covered entities' data practices. Similarly, public health entities could face new impediments partnering with private sector businesses and organizations if future rules restrict the use and disclosure of information for public health purposes. (See Section V.A and V.B.5). Some unintended consequences could be mitigated by early communication between HHS and FTC to ensure that proposed rules consider the health perspectives and objectives. If FTC promulgates new regulations on commercial surveillance, joint guidance by the FTC and HHS might be needed to ensure that HIPAA covered entities understand their compliance obligations under both laws. A future NCVHS convening could explore the following issues:

- Whether timely comments or input could inform or assist the FTC rulemaking process related to:
    - Beneficial health-related data practices that could be impeded by future FTC rules, including learning health systems, precision public health, and private sector assistance in public health surveillance.
    - Harmful health-related data practices that could be considered as the subject of future FTC restrictions.
    - Conflicts between proposed FTC rules and existing legal privacy frameworks for health data.
    - Consideration of rules that address potential the group harms in addition to individual harms. (See Sections III.A., IV.B, V.E, V.F.1, V.F.3)

VII. REFERENCES

1. National Committee on Vital & Health Statistics. Request for Environmental Scan on Current and Potential Privacy, Confidentiality and Security Policies and Issues.

2. Lively TK. US State Privacy Legislation Tracker. IAPP. Published August 11, 2022. Accessed September 17, 2022. https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

3. Uniform Law Commission. *Uniform Personal Data Protection Act* .; 2021. Accessed August 2, 2021. https://www.uniformlaws.org/committees/community-home?CommunityKey=28443329-e343-4cbc-8c72-60b12fd18477

4. Fazlioglu M. US Federal Privacy Legislation Tracker: Introduced in the 117th Congress (2021-2022). IAPP.org. Published May 31, 2022. Accessed August 29, 2022. https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf

5. Office of the National Coordinator for Health Information Technology T. *21ST CENTURY CURES ACT: INTEROPERABILITY, INFORMATION BLOCKING, AND THE ONC HEALTH IT CERTIFICATION PROGRAM PROPOSED RULE Seven Exceptions to the Information Blocking Provision*. Accessed September 3, 2019. https://www.healthit.gov/sites/default/files/nprm/ONCCuresNPRMInfoBlocking.pdf

6. The American Data and Privacy Protection Act deserves a vote - The Washington Post. *Washington Post*. https://www.washingtonpost.com/opinions/2022/08/07/federal-privacy-legislation-deserves-vote/. Published August 7, 2022. Accessed September 17, 2022.

7. *American Data Privacy & Protection Act (ADPPA), H.R. 8152*.; 2022.

8. Gold A. Pelosi rejects bipartisan privacy bill. Axios. Published September 1, 2022. Accessed September 17, 2022. https://www.axios.com/2022/09/01/pelosi-rejects-bipartisan-privacy-bill

9. Curran C, Schmit C. *The ADPPA — Possible Issues For Public Health* .; 2022. Accessed September 17, 2022. https://docs.google.com/document/d/1T7tBnlUaqJd8bet7ZpIINo-MCp7r4Z9UQXp6w_2Esys/edit

10. Solow-Niederman A. Information Privacy and the Inference Economy. *SSRN Electronic Journal*. Published online September 10, 2021. doi:10.2139/SSRN.3921003

11. Schmit CD, Doerr MJ, Wagner JK. Leveraging IP for AI governance. *Science (1979)*. 2023;379(6633):646-648. doi:10.1126/science.add2202

12. O'Neil C. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown; 2016. Accessed July 11, 2017. https://books.google.com/books/about/Weapons_of_Math_Destruction.html?id=NRC9jwEACAAJ&hl=en

13. Report: Algorithms Are Worsening Racism, Bias, Discrimination. Public Citizen. Published 2021. Accessed September 19, 2022.

https://www.citizen.org/news/report-algorithms-are-worsening-racism-bias-discrimination/

14. Noble SU·. *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press; 2018.

15. Köchling A, Wehner MC. Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development. *Business Research*. 2020;13(3):795-848. doi:10.1007/S40685-020-00134-W/FIGURES/2

16. Kwok R. Can Bias Be Eliminated from Algorithms? Yale Insights. Published November 24, 2021. Accessed September 19, 2022. https://insights.som.yale.edu/insights/can-bias-be-eliminated-from-algorithms

17. Turner Lee N. Detecting racial bias in algorithms and machine learning. *Journal of Information, Communication and Ethics in Society*. 2018;16(3):252-260. doi:10.1108/JICES-06-2018-0056/

18. Acemoglu D. *Harms of AI.*; 2021.

19. Braveman P, Gottlieb L. The Social Determinants of Health: It's Time to Consider the Causes of the Causes. *Public Health Reports*. 2014;129(1_suppl2):19-31. doi:10.1177/00333549141291S206

20. Galea S, Tracy M, Hoggatt KJ, Dimaggio C, Karpati A. Estimated deaths attributable to social factors in the United States. *Am J Public Health*. 2011;101(8):1456-1465. doi:10.2105/AJPH.2010.300086

21. Wachter S. The Theory of Artificial Immutability: Protecting Algorithmic Groups Under Anti-Discrimination Law. *Tulane Law Rev*. 2022;97. doi:10.48550/arxiv.2205.01166

22. St. John P. The untold story of how the Golden State Killer was found. *Los Angeles Times*. https://www.latimes.com/california/story/2020-12-08/man-in-the-window. Published December 8, 2020. Accessed September 17, 2022.

23. Dobbs v. Jackson, 142 S.Ct. 2228 . Published online 2022.

24. Burke G, Dearen J. Tech tool offers police 'mass surveillance on a budget' | AP News. *AP*. https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef. Published September 2, 2022. Accessed September 5, 2022.

25. Cohen JE. How (Not) to Write a Privacy Law . Knight First Amendment Institute at Columbia University. Published March 23, 2021. Accessed January 26, 2022. https://knightcolumbia.org/content/how-not-to-write-a-privacy-law

26. Hulkower R, Penn M, Schmit C. Privacy and Confidentiality of Public Health Information. In: Magnuson JA, Dixon BE, eds. *Public Health Informatics and Information Systems, 3rd Edition*. Health Informatics. Springer London; 2020:147-166. doi:10.1007/978-3-030-41215-9_9

27. Schmit C, Sunshine G, Pepin D, Ramanathan T, Menon A, Penn M. Transitioning From Paper to Digital: State Statutory and Regulatory Frameworks for Health Information

Technology. *Public Health Reports*. 2017;132(5):585-592. doi:10.1177/0033354917722994

28. Schmit C, Larson B, Kum HC. Data Privacy in the Time of Plague. *Yale J Health Policy Law Ethics*. 2022;21(1):152-227. doi:10.2139/SSRN.3968130

29. Duball J. Uniform Law Commission takes up privacy law endeavor. IAPP. Published February 25, 2020. Accessed September 19, 2022. https://iapp.org/news/a/uniform-law-commission-takes-up-privacy-law-endeavor/

30. Klosowski T. The State of Consumer Data Privacy Laws in the US (And Why It Matters) | Wirecutter. The New York Times Wirecutter. Published September 6, 2021. Accessed September 19, 2022. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

31. Solove D, Hartzog W. The FTC and the new common law of privacy. *Colum L Rev*. Published online 2014. Accessed July 27, 2017. http://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/clr114&section=19

32. Maass P. Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless. WIRED. Published June 28, 2012. Accessed September 19, 2022. https://www.wired.com/2012/06/ftc-fail/

33. Moshell R. ... And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection., . *Tex Tech L Rev* . 2005;37:357.

34. Parasidis E, Pike E, McGraw D. A Belmont Report for Health Data. *New England Journal of Medicine*. 2019;380(16):1493-1495. doi:10.1056/NEJMp1816373

35. Schuler K. Federal data privacy regulation is on the way — That's a good thing. IAPP. Published January 22, 2022. Accessed September 19, 2022. https://iapp.org/news/a/federal-data-privacy-regulation-is-on-the-way-thats-a-good-thing/

36. Crenshaw J. It's Time to Get Serious About National Data Privacy Legislation | U.S. Chamber of Commerce. U.S. Chamber of Commerce. Published January 28, 2022. Accessed September 19, 2022. https://www.uschamber.com/technology/data-privacy/its-time-to-get-serious-about-national-privacy-legislation

37. Walker K. The urgent necessity of enacting a national privacy law. Google, The Keyword. Published April 25, 2022. Accessed September 19, 2022. https://blog.google/outreach-initiatives/public-policy/the-urgent-necessity-of-enacting-a-national-privacy-law/

38. Kimball S. Facebook CEO Zuckerberg backs tighter Internet privacy and election laws. CNBC. Published 2019. Accessed May 7, 2019. https://www.cnbc.com/2019/03/30/mark-zuckerberg-calls-for-tighter-internet-regulations-we-need-a-

more-active-role-for-governments.html

39. Pichai S. Privacy Should Not Be a Luxury Good. The New York Times. Published 2019. Accessed May 21, 2019. https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html?smid=nytcore-ios-share

40. Schmit C, Giannouchos T, Ramezani M, Zheng Q, Morrisey M, Kum HC. US Privacy Laws Go Against Public Preferences: Impeding Public Health and Research (Preprint). *J Med Internet Res*. 2020;23(7):e25266. doi:10.2196/25266

41. About – National Committee on Vital and Health Statistics. ncvhs.hhs.gov/. Accessed September 20, 2022. https://ncvhs.hhs.gov/about/

42. National Committee on Vital and Health Statistics. NCVHS Strategic Plan. ncvhs.hhs.gov. Published 2017. Accessed September 20, 2022. https://ncvhs.hhs.gov/strategic_plans/september-13-2017-ncvhs-strategic-plan/

43. *California Consumer Privacy Act, 2018 Cal. Legis. Serv. Ch. 55 (A.B. 375) (West).*; 2018.

44. *2018 Cal. Legis. Serv. Ch. 735 (S.B. 1121) (West).*; 2018.

45. *2019 Cal. Legis. Serv. Ch. 757 (A.B. 1355) (West).*; 2019.

46. *California Privacy Rights Act of 2020, 2020 Cal. Legis. Serv. Prop. 24 (West).*; 2020. Accessed September 3, 2022. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

47. *California Privacy Rights Act of 2020, § 140(d)(1).*; 2020.

48. *California Privacy Rights Act of 2020, § 145.*; 2020.

49. *California Privacy Rights Act of 2020, § 140(v).*; 2020.

50. *California Privacy Rights Act of 2020, § 146(a).*; 2020.

51. *California Privacy Rights Act of 2020, § 140(Ae).*; 2020.

52. *California Privacy Rights Act of 2020, § 121.*; 2020.

53. *California Privacy Rights Act of 2020, § 135.*; 2020.

54. *California Privacy Rights Act of 2020, § 100(c).*; 2020.

55. *California Privacy Rights Act of 2020, § 120.*; 2020.

56. *California Privacy Rights Act of 2020, § 150(a).*; 2020.

57. *California Privacy Rights Act of 2020, § 155(a).*; 2020.

58. *The California Age-Appropriate Design Code Act, AB-2273* .; 2022. Accessed September 17, 2022. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB2273

59. Thompson D. California 1st with law protecting children's online privacy. AP News. Published September 15, 2022. Accessed September 17, 2022. https://apnews.com/article/technology-health-gavin-newsom-data-privacy-government-and-politics-

b4767350cfe67fe45b44b03b713f0c22

60. *Colorado Privacy Act, 2021 Colo. Legis. Serv. Ch. 21-190 (West).*; 2021.

61. *Colorado Privacy Act § 1304.*; 2021.

62. *Colorado Privacy Act § 1308(1).*; 2021.

63. *Colorado Privacy Act § 1308(2).*; 2021.

64. *Colorado Privacy Act § 1308(3).*; 2021.

65. *Colorado Privacy Act § 1308(4).*; 2021.

66. *Colorado Privacy Act § 1308(6).*; 2021.

67. *Colorado Privacy Act § 1308(7).*; 2021.

68. *Colorado Privacy Act § 1306(1)(a)(i).*; 2021.

69. *Colorado Privacy Act § 1303(24).*; 2021.

70. *Colorado Privacy Act § 1309(1),(2).*; 2021.

71. *Colorado Privacy Act § 1304(3)(a)(XI).*; 2021.

72. *Colorado Privacy Act § 1311(1).*; 2021.

73. *Connecticut Data Privacy Act § 1.*; 2022.

74. *Connecticut Data Privacy Act § 2.*; 2022.

75. *Connecticut Data Privacy Act § 4.*; 2022.

76. *Connecticut Data Privacy Act § 5.*; 2022.

77. *Connecticut Data Privacy Act § 6.*; 2022.

78. *Connecticut Data Privacy Act § 8.*; 2022.

79. *Connecticut Data Privacy Act § 7.*; 2022.

80. *Connecticut Data Privacy Act § 11.*; 2022.

81. *Utah Consumer Privacy Act, S.B. 227.*; 2022.

82. *Utah Consumer Privacy Act § 101.*; 2021.

83. *Utah Consumer Privacy Act § 102.*; 2021.

84. *Utah Consumer Privacy Act § 103.*; 2021.

85. *Utah Consumer Privacy Act § 301.*; 2021.

86. *Utah Consumer Privacy Act § 302.*; 2021.

87. *Utah Consumer Privacy Act § 302(4).*; 2021.

88. *Utah Consumer Privacy Act § 401.*; 2021.

89. *Utah Consumer Privacy Act § 402.*; 2021.

90. *Utah Consumer Privacy Act § 403.*; 2021.

91. *Utah Consumer Privacy Act § 305.*; 2021.

92. *Consumer Data Protection Act, 2021 Va. Legis. Serv. 1st Sp. Sess., Ch. 36*

(S.B. 1392).; 2022. Accessed September 4, 2022. https://lis.virginia.gov/cgi-bin/legp604.exe?212+ful+CHAP0035

93. *Virginia Consumer Data Protection Act § 572*.; 2022.

94. *Virginia Consumer Data Protection Act § 572(A)*.; 2022.

95. *Virginia Consumer Data Protection Act § 572(B)*.; 2022.

96. *Virginia Consumer Data Protection Act § 573*.; 2022.

97. *Virginia Consumer Data Protection Act § 574*.; 2022.

98. *Virginia Consumer Data Protection Act § 571*.; 2022.

99. *Virginia Consumer Data Protection Act § 574(A)*.; 2022.

100. *Virginia Consumer Data Protection Act § 576(A)*.; 2022.

101. *Virginia Consumer Data Protection Act § 580*.; 2022.

102. *Michigan Consumer Privacy Act, House Bill 5989* .; 2022. Accessed September 17, 2022. https://www.legislature.mi.gov/(S(oj1v1sjn1vlxa05d1emsfz1u))/mileg.aspx?page=getobject&objectname=2022-HB-5989&query=on

103. *Michigan Consumer Privacy Act § 5*.; 2022.

104. *Michigan Consumer Privacy Act § 3*.; 2022.

105. *Michigan Consumer Privacy Act § 9*.; 2022.

106. *Michigan Consumer Privacy Act § 11*.; 2022.

107. *Michigan Consumer Privacy Act § 1*.; 2022.

108. *Michigan Consumer Privacy Act § 13*.; 2022.

109. *New Jersey Disclosure and Accountability Transparency Act, Bill A505e*.; 2022. Accessed September 17, 2022. https://www.njleg.state.nj.us/bill-search/2022/A505

110. *NJ DaTA § 3*.; 2022.

111. *NJ DaTA § 23*.; 2022.

112. *NJ DaTA § 7,8,11*.; 2022.

113. *NJ DaTA § 5*.; 2022.

114. *NJ DaTA § 13,17*.; 2022.

115. *NJ DaTA § 18,20*.; 2022.

116. *NJ DaTA § 4*.; 2022.

117. *NJ DaTA § 6*.; 2022.

118. *Ohio Personal Privacy Act, House Bill 376* .; 2022. Accessed September 17, 2022. https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA134-HB-376

119. *Ohio Personal Privacy Act § 1355.02*.; 2022.

120. *Ohio Personal Privacy Act § 1355.03-.09*.; 2022.

121. *Ohio Personal Privacy Act § 1355.10*.; 2022.

122. *Ohio Personal Privacy Act § 1355.11*.; 2022.

123. *Pennsylvania Consumer Data Protection Act, House Bill 2257*. PA General Assembly; 2022. Accessed September 17, 2022. https://www.legis.state.pa.us/cfdocs/billinfo/billinfo.cfm?syear=2021&sind=0&body=H&type=B&bn=2257

124. *Consumer Data Privacy Act, House Bill 2202*. PA General Assembly; 2022. Accessed September 17, 2022. https://www.legis.state.pa.us/cfdocs/billInfo/billInfo.cfm?sYear=2021&sInd=0&body=h&type=b&bn=2202

125. *Consumer Data Privacy Act, House Bill 1126*. PA General Assembly; 2022. Accessed September 17, 2022. https://www.legis.state.pa.us/cfdocs/billinfo/bill_history.cfm?syear=2021&sind=0&body=H&type=B&bn=1126

126. *H.B. 1126 § 2.*; 2022.

127. *H.B. 1126 § 4.*; 2022.

128. *H.B. 1126 § 4(n),(o).*; 2022.

129. *H.B. 1126 § 4(p).*; 2022.

130. *H.B. 2202 § 2.*; 2022.

131. *H.B. 2202 § 3(a).*; 2022.

132. *H.B. 2202 § 3(b)(k).*; 2022.

133. *H.B. 2202 § 3(e).*; 2022.

134. *H.B. 2202 § 3(f).*; 2022.

135. *H.B. 2202 § 3(g).*; 2022.

136. *H.B. 2202 § 3(h),(i).*; 2022.

137. *H.B. 2202 § 3(b).*; 2022.

138. *H.B. 2202 § 3(d).*; 2022.

139. *H.B. 2202 § 3(l).*; 2022.

140. *H.B. 2202 § 3(k).*; 2022.

141. *H.B. 2202 § 3(m).*; 2022.

142. *Consumer Data Protection Act § 103.*; 2022.

143. *Consumer Data Protection Act § 103(b) .*; 2022.

144. *Consumer Data Protection Act § 103(c).*; 2022.

145. *Consumer Data Protection Act § 102.*; 2022.

146. *Consumer Data Protection Act § 301 .*; 2022.

147. *Consumer Data Protection Act § 306(f).*; 2022.

148. *Consumer Data Protection Act § 304.*; 2022.

149. *Consumer Data Protection Act § 501*.

150. *Consumer Data Protection Act § 502.*; 2022.

151. *Consumer Data Protection Act § 503.*; 2022.

152. *UPDPA § 3(a).*; 2021.

153. *UPDPA § 3(b).*; 2021.

154. *UPDPA § 3(c).*; 2021.

155. *UPDPA § 7.*; 2021.

156. *UPDPA § 8.*; 2021.

157. *UPDPA § 9.*; 2021.

158. Solove D. A Critique of the Uniform Law Commission's Uniform Personal Data Protection Act - TeachPrivacy. Teach Privacy. Published February 19, 2022. Accessed August 30, 2022. https://teachprivacy.com/a-critique-of-the-uniform-law-commissions-

uniform-personal-data-protection-act/

159. Marchant GE, Abbott KW, Allenby B, eds. *Innovative Governance Models for Emerging Technologies*. Edward Elgar Publishing Inc.; 2014.

160. *UPDPA § 12-15*.; 2021.

161. Trade Regulation Rule on Commercial Surveillance and Data Security. Federal Register. Published August 22, 2022. Accessed September 18, 2022. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

162. Black JR, Hulkower RL, Ramanathan T. Health Information Blocking: Responses Under the 21st Century Cures Act. *Public Health Reports*. 2018;133(5):610-613. doi:10.1177/0033354918791544

163. The Office of the National Coordinator for Health Information Technology. *REPORT TO CONGRESS, APRIL 2015 - Report on Health Information Blocking*.; 2015.

164. *45 CFR § 171.200-303* .; 2020.

165. *ADPPA § 2(29)*.; 2022.

166. *ADPPA § 302(d)(1)*.; 2022.

167. *ADPPA § 402*.; 2022.

168. *ADPPA § 101(b)*.; 2022.

169. *ADPPA §§ 201-210*.; 2022.

170. *ADPPA § 102*.; 2022.

171. *ADPPA § 2(28)*.; 2022.

172. *ADPPA § 401*.; 2022.

173. *ADPPA § 403*.; 2022.

174. *ADPPA § (2)(12)* .; 2022.

175. Full Committee Meeting, Transcript-July 21, 2022. Presented at: July 21, 2022.

176. Catron E, Kibel G. Federal data privacy legislation: Differences with state laws raise preemption issues | Reuters. Reuters. Published August 10, 2022. Accessed September 17, 2022. https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10/

177. *ADPPA § 404*.; 2022.

178. Kaye. Kate. The FTC's new enforcement weapon spells death for algorithms. Protocol. Published March 14, 2022. Accessed August 28, 2022. https://www.protocol.com/policy/ftc-algorithm-destroy-data-privacy

179. Xafis V, Schaefer GO, Labude MK, et al. An Ethics Framework for Big Data in Health and Research. *Asian Bioeth Rev*. 2019;11(3):227-254. doi:10.1007/S41649-019-00099-X/TABLES/7

180. Federal Trade Commission. *Data Brokers A Call for Transparency and Accountability*.; 2014.

181. Kody H. Standing to Challenge Familial Searches of Commercial DNA Databases. *William Mary Law Rev*. 2019;61(1). Accessed September 17, 2022.

https://scholarship.law.wm.edu/wmlr/vol61/iss1/7

182. Brodkin J. San Francisco sued by woman who says her rape-kit DNA was used to arrest her . Ars Technica. Published September 14, 2022. Accessed September 16, 2022. https://arstechnica.com/tech-policy/2022/09/lawsuit-sfpd-used-victims-dna-from-rape-kit-exam-to-arrest-her-for-burglary/

183. Krishnan A, Cohen K, Hackley C. Digital Privacy in the Post-Dobbs Landscape | The Regulatory Review. The Regulatory Review. Published August 27, 2022. Accessed September 18, 2022. https://www.theregreview.org/2022/08/27/saturday-seminar-digital-privacy-in-the-post-dobbs-landscape/

184. HHS Office for Civil Rights. HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care. HHS.gov. Published 2022. Accessed September 18, 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html

185. Spector-Bagdady K, Mello MM. Protecting the Privacy of Reproductive Health Information After the Fall of Roe v Wade. *JAMA Health Forum*. 2022;3(6):e222656-e222656. doi:10.1001/JAMAHEALTHFORUM.2022.2656

186. Cameron D. FTC Members Unanimously Press Congress for Tough National Privacy Protections. Gizmodo. Published 2019. Accessed May 21, 2019. https://gizmodo.com/ftc-members-unanimously-press-congress-for-tough-nation-1834624258

187. Cameron D, Leffer L. Border Agents Surveil Americans' Phones Without Warrants: Wyden. Gizmodo. Published September 15, 2022. Accessed September 16, 2022. https://gizmodo.com/border-patrol-surveillance-cell-data-no-warrants-1849540504?utm_medium=sharefromsite%26utm_source=_email&utm_campaign=top

188. *General Data Protection Regulation (GDPR)*.

189. Balkin JM. Information Fiduciaries and the First Amendment. *UC Davis Law Review*. 2015;49. Accessed August 29, 2022. https://heinonline.org/HOL/Page?handle=hein.journals/davlr49&id=1203&div=&collection=

190. Balkin JM. The Fiduciary Model of Privacy. *Harvard Law Review Forum*. 2020;134. Accessed August 29, 2022. https://heinonline.org/HOL/Page?handle=hein.journals/forharoc134&id=11&div=4&collection=journals

191. Richards NM, Hartzog W. A Duty of Loyalty for Privacy Law. *SSRN Electronic Journal*. Published online July 3, 2020. doi:10.2139/SSRN.3642217

192. Khan LM, Pozen DE. A Skeptical View of Information Fiduciaries. *Harv Law Rev*. 2019;133. Accessed August 29, 2022. https://heinonline.org/HOL/Page?handle=hein.journals/hlr133&id=508&div=31&collection=journals

193. van Loo R. The New Gatekeepers: Private Firms as Public Enforcers. *Va Law Rev*. 2020;106:467. Accessed August 30, 2022. https://www.virginialawreview.org/articles/new-gatekeepers-private-firms-public-enforcers/

194. Ohm P. Regulating at Scale. *Georgetown Law Technology Review*. 2018;2:546. Accessed August 29, 2022. https://perma.cc/VVY9-8PPT]

195. Holland M. Federal data privacy legislation could benefit U.S. economy. TechTarget. Published June 21, 2021. Accessed September 19, 2022. https://www.techtarget.com/searchcio/news/252502418/Federal-data-privacy-legislation-could-benefit-US-economy

196. Office for Civil Rights H. *Personal Health Records and the HIPAA Privacy Rule*.

197. Emerson J. No, HIPAA doesn't apply to employers, businesses asking for vaccination status | WKRC. WICS/WRSP. Published May 20, 2021. Accessed September 19, 2022. https://local12.com/news/nation-world/no-hipaa-doesnt-apply-to-employers-businesses-asking-for-vaccination-status-05-20-2021

198. Singer N. In Privacy Laws, an Incomplete American Quilt - The New York Times. The New York Times. Published March 30, 2013. Accessed September 19, 2022. https://www.nytimes.com/2013/03/31/technology/in-privacy-laws-an-incomplete-american-quilt.html

199. Schmit C. Federal Privacy Laws. The Network for Public Health Law. Published 2019. Accessed May 22, 2019. https://www.networkforphl.org/resources/topics__resources/health_information_and_data_sharing/federal_privacy_laws/

200. Schmit C, Kelly K, Bernstein J. Cross Sector Data Sharing: Necessity, Challenge, and Hope. *Journal of Law, Medicine & Ethics*. 2019;47(S2):83-86. doi:10.1177/1073110519857325

201. Woods WJ, Dilley JW, Lihatsh T, Sabatino J, Adler B, Rinaldi J. Name-based reporting of HIV-positive test results as a deterrent to testing. *https://doi.org/102105/AJPH8971097*. 2011;89(7):1097-1100. doi:10.2105/AJPH.89.7.1097

202. Cederbaum J. Name-Based HIV Reporting: Current Status and Advocacy Needs. *Journal of HIV/AIDS & Social Services* . 2008;7(2):117-133. doi:10.1080/15381500802006474

203. Doughty R. The Confidentiality of HIV-Related Information: Responding to the Resurgence of Aggressive Public Health Interventions in the AIDS Epidemic. *Calif Law Rev*. 1994;82(1):111-184. Accessed June 7, 2017. http://www.jstor.org/stable/3480851

204. Urban Indian Health Institute. *Data Genocide of American Indians and Alaska Natives in COVID-19 Data*.; 2021. Accessed August 12, 2022. https://www.uihi.org/projects/data-genocide-of-american-indians-and-alaska-natives-in-covid-19-data/

205. Fairchild AL, Bayer Ronald, Colgrove JKeith, Wolfe D. *Searching Eyes :*

Privacy, the State, and Disease Surveillance in America. University of California Press; 2007.

206. Fairchild AL. The Right to Know, The Right to be Counted, The Right to Resist: Cancer, AIDS, and the Politics of Privacy and Surveillance in Post-War America. *J Med Law Ethics*. 2015;3(1):45-64. doi:10.7590/221354015X14319325750034

207. Kern R. Bipartisan draft bill breaks stalemate on federal data privacy negotiations. *POLITICO*. https://www.politico.com/news/2022/06/03/bipartisan-draft-bill-breaks-stalemate-on-federal-privacy-bill-negotiations-00037092. Published June 3, 2022. Accessed June 9, 2022.

208. *UPDPA § 11*.; 2021.

209. Prosperi M, Min JS, Bian J, Modave F. Big data hurdles in precision medicine and precision public health. *BMC Medical Informatics and Decision Making 2018 18:1*. 2018;18(1):1-15. doi:10.1186/S12911-018-0719-2

210. Rasmussen SA, Khoury MJ, Rio C del. Precision Public Health as a Key Tool in the COVID-19 Response. *JAMA*. 2020;324(10):933-934. doi:10.1001/JAMA.2020.14992

211. Dolley S. Big data's role in precision public health. *Front Public Health*. 2018;6:68. doi:10.3389/FPUBH.2018.00068/BIBTEX

212. Bennett KJ, Olsen JM, Harris S, Mekaru S, Livinski AA, Brownstein JS. The Perfect Storm of Information: Combining Traditional and Non-Traditional Data Sources for Public Health Situational Awareness During Hurricane Response. *PLoS Curr*. 2013;5(DEC). doi:10.1371/CURRENTS.DIS.D2800AA4E536B9D6849E966E91488003

213. Stein D, Handspicker B, Bishop M, et al. *Modernizing Consent to Advance Health and Equity*.; 2021.

214. van Panhuis WG, Paul P, Emerson C, et al. A systematic review of barriers to data sharing in public health. *BMC Public Health*. 2014;14(1):1144. doi:10.1186/1471-2458-14-1144

215. Public Health Informatics Institute. *Toolkit for Planning an EHR-Based Surveillance Program*.; 2021. Accessed August 12, 2022. https://phii.org/course/toolkit-for-planning-an-ehr-based-surveillance-program/

216. Chatham House. Strengthening Data Sharing for Public Health. The Royal Institute of International Affairs. Published 2017. Accessed August 11, 2021. https://www.chathamhouse.org/about-us/our-departments/global-health-programme/strengthening-data-sharing-public-health

217. Wachter RM, Cassel CK. Sharing Health Care Data with Digital Giants: Overcoming Obstacles and Reaping Benefits while Protecting Patients. *JAMA - Journal of the American Medical Association*. 2020;323(6):507-508. doi:10.1001/JAMA.2019.21215

218. Amann J, Vetter D, Blomberg SN, et al. To explain or not to explain?—Artificial intelligence explainability in clinical decision support systems.

PLOS Digital Health. 2022;1(2):e0000016. doi:10.1371/JOURNAL.PDIG.0000016

219. Brass EP. The Gap Between Clinical Trials and Clinical Practice: The Use of Pragmatic Clinical Trials to Inform Regulatory Decision Making. *Clin Pharmacol Ther*. 2010;87(3):351-355. doi:10.1038/clpt.2009.218

220. Etheredge LM. A Rapid-Learning Health System. *Health Aff*. 2007;26(Suppl1):w107-w118. doi:10.1377/hlthaff.26.2.w107

221. Gonzalez-SmithJonathan, ShenHumphrey, SingletaryElizabeth, SilcoxChristina. How Health Systems Decide to Use Artificial Intelligence for Clinical Decision Support. *NEJM Catal Innov Care Deliv*. 2022;3(4). doi:10.1056/CAT.21.0416

222. Krumholz HM, Terry SF, Waldstreicher J. Data Acquisition, Curation, and Use for a Continuously Learning Health System. *JAMA*. 2016;316(16):1669. doi:10.1001/jama.2016.12537

223. Medicine I of. *The Learning Healthcare System*. National Academies Press; 2007. doi:10.17226/11903

224. Spector-Bagdady K, Jagsi R. Big data, ethics, and regulations: Implications for consent in the learning health system. *Med Phys*. 2018;45(10):e845. doi:10.1002/MP.12707

225. Bowman DM. The hare and the tortoise: an Australian perspective on regulating new technologies and their products and processes. In: *Innovative Governance Models for Emerging Technologies*. Edward Elgar Publishing; :155-175. doi:10.4337/9781782545644.00015

226. Mandel G. Regulating emerging technologies. *Law Innov Technol*. 2009;1(1):75-92. Accessed December 19, 2016. http://www.tandfonline.com/doi/pdf/10.1080/17579961.2009.11428365

227. Marchant GE, Abbott KW, Allenby BR, eds. *Innovative Governance Models for Emerging Technologies*. Edward Elgar Publishing; 2013.

228. Giordano C, Brennan M, Mohamed B, Rashidi P, Modave F, Tighe P. Accessing Artificial Intelligence for Clinical Decision-Making. *Front Digit Health*. 2021;3:65. doi:10.3389/FDGTH.2021.645232/XML/NLM

229. Access Now, ADL (Anti-Defamation League), Americans for Democratic Action (ADA), et al. Letter to Nancy Pelosi, RE: Move H.R. 8152, the American Data Privacy and Protection Act. civilrightsdocs.info. Published August 25, 2022. Accessed September 1, 2022. https://civilrightsdocs.info/pdf/policy/letters/2022/Coalition-Letter-Supporting-ADPPA_August-2022.pdf

230. Kum HC, Krishnamurthy A, Machanavajjhala A, Ahalt SC. Social genome: Putting big data to work for population informatics. *Computer (Long Beach Calif)*. 2014;47(1):56-63. doi:10.1109/MC.2013.405

231. Frakt AB, Bagley N. Protection or Harm? Suppressing Substance-Use Data. *New England Journal of Medicine*. 2015;372(20):1879-1881. doi:10.1056/NEJMp1501362

232. Bambauer J, Ray B. *COVID-19 Apps Are Terrible—They Didn't Have to Be*.; 2020. Accessed September 1, 2022. https://www.lawfareblog.com/covid-19-apps-are-terrible-they-didnt-have-be

233. Rozenshtein AZ. Digital Disease Surveillance. *American University Law Review*. 2020;70:1511-1575. Accessed January 25, 2022. https://www.lawfareblog.com/covid-19-

234. World Health Organization. *WHO Guidelines on Ethical Issues in Public Health Surveillance*.; 2017. Accessed July 9, 2017. http://apps.who.int/iris/bitstream/10665/255721/1/9789241512657-eng.pdf

235. Bayer R, Fairchild AL. The Genesis of Public Health Ethics. *Bioethics*. 2004;18(6). doi:10.1111/j.1467-8519.2004.00412.x

236. Lee LM, Heilig CM, White A. Ethical Justification for Conducting Public Health Surveillance Without Patient Consent. *Am J Public Health*. 2012;102(1):38. doi:10.2105/AJPH.2011.300297

237. Kass NE. An Ethics Framework for Public Health. *Am J Public Health*. 2001;91(11):1776-1782. doi:10.2105/AJPH.91.11.1776

238. Langat P, Pisartchik D, Silva D, et al. Is There a Duty to Share? Ethics of Sharing Research Data in the Context of Public Health Emergencies. *Public Health Ethics*. 2011;4(1):4-11. doi:10.1093/PHE/PHR005

239. Ballantyne A. Adjusting the focus: A public health ethics approach to data research. *Bioethics*. 2019;33(3):357-366. doi:10.1111/BIOE.12551

240. Lee LM. Public Health Ethics Theory: Review and Path to Convergence. *Journal of Law Medicine & Ethics*. Published online 2012:85-98. doi:10.1111/j.1748-720X.2012.00648.x

241. Council for International Organizations of Medical Sciences. *International Guidelines for Ethical Review of Epidemiological Studies*.; 1991.

242. Shaw JA, Sethi N, Cassel CK. Social license for the use of big data in the COVID-19 era. *npj Digital Medicine 2020 3:1*. 2020;3(1):1-3. doi:10.1038/s41746-020-00342-y

243. Jijelava D, Vanclay F. Legitimacy, credibility and trust as the key components of a social licence to operate: An analysis of BP's projects in Georgia. *J Clean Prod*. 2017;140:1077-1086. doi:10.1016/J.JCLEPRO.2016.10.070

244. Dickert N, Sugarman J. Ethical goals of community consultation in research. *Am J Public Health*. 2005;95(7):1123-1127. doi:10.2105/AJPH.2004.058933

245. Corscadden K, Wile A, Yiridoe E. Social license and consultation criteria for community wind projects. *Renew Energy*. 2012;44:392-397. doi:10.1016/J.RENENE.2012.02.009

246. Hospital Accused On Cancer Study; Live Cells Given to Patients Without Their Consent, Director Tells Court; Allegation is Denied; Chronic Disease

Institution Defends Action—Value of Tests Is Praised. *The New York Times*. https://www.nytimes.com/1964/01/21/archives/hospital-accused-on-cancer-study-live-cells-given-to-patients.html. Published January 21, 1964. Accessed September 1, 2022.

247. Permissible Medical Experiments (The Nuremberg Code). *Trials of War Criminals before the Nuremberg Military Tribunals under Control Council Law*. 1949;2(10):181-182. Accessed July 23, 2017. http://www.eddatatraining.net/assets/documents/ethics-references.pdf

248. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *The Belmont Report*.; 1979. Accessed September 5, 2019. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

249. Reimann M. Willowbrook, the institution that shocked a nation into changing its laws. Timeline. Published June 14, 2017. Accessed September 1, 2022. https://timeline.com/willowbrook-the-institution-that-shocked-a-nation-into-changing-its-laws-c847acb44e0d

250. World Medical Assembly. *Declaration of Helsinki: Recommendations Guiding Doctors in Clinical Research*.; 1964.

251. Schmit CD, Willis B, McCall H, Altabbaa A, Washburn D. Views on Increased Federal Access to State and Local National Syndromic Surveillance Program Data: A Nominal Group Technique Study with State and Local Epidemiologists. *BMC Public Health*. 2023;23(1). doi:https://doi.org/10.1186/s12889-023-15161-5

252. Schmit C, Willis B, Teel E, Washburn D. *Review of Federal Access Policies for State National Syndromic Surveillance Program Data: Findings and Implementation Strategies*.; 2023. Accessed February 22, 2023. https://cdn.ymaws.com/www.cste.org/resource/resmgr/pdfs/Review_of_Federal_Access_Pol.pdf

253. Schmit C, Willis B, Teel E, Washburn D. Federal Access Policy for State National Syndromic Surveillance Program Data: Findings and Recommendations. In: *CSTE 2022 Annual Conference*. ; 2022.

254. Centers for Disease Control and Prevention National Syndromic Surveillance Program Data Sharing and Use Agreement. Published online March 20, 2018. Accessed February 10, 2022. https://docs.google.com/document/d/1JB9V0l6Pv1TXrhgaQXiy7EBaIi9XtR-m/edit

255. Schmit CD, Willis B, Teel E. Intractable? Identifying Consensus Policy Opportunities to Address Legal and Ethical Challenges in National Public Health Surveillance from State and Local Epidemiologist Leaders. In: *APHA 2022 Annual Meeting and Expo*. ; 2022. Accessed December 28, 2022. https://oaktrust.library.tamu.edu/handle/1969.1/196995

256. National Syndromic Surveillance Program Community of Practice. *April 2020 NSSP Community of*

Practice Call.; 2020. Accessed December 27, 2022. https://knowledgerepository.syndromicsurveillance.org/community-practice-monthly-calls

257. van Panhuis WG, Paul P, Emerson C, et al. A systematic review of barriers to data sharing in public health. *BMC Public Health*. 2014;14(1):1-9. doi:10.1186/1471-2458-14-1144/TABLES/1

258. Ohm P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review*. 2010;57:1701.

259. Office for Civil Rights. *Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*.; 2012.

260. Stead WW. *Recommendations on De-Identification of Protected Health Information under HIPAA*.; 2017. Accessed September 5, 2022. http://www.ncvhs.hhs.gov/transcripts-

261. Kendall S, Lobuglio D, eds. *Location Data in the Context of Public Health, Research, and Law Enforcement: An Exploration of Governance Frameworks*. National Academies Press; 2022. doi:10.17226/26645

262. Medeiros CB, Kum HC, Sandin S, et al. *Integrating Knowledge from the Individual to the Population Level Data* .; 2022.

263. Raab CD. The Distribution of Privacy Risks: Who Needs Protection? *the Information Society*. 1998;14(4):263-274. doi:10.1080/019722498128719

264. Chander A, Kaminski M, McGeveran W. Catalyzing Privacy Law. *Georgetown Law Faculty Publications and Other Works*. Published online August 7, 2019. Accessed January 26, 2022. https://scholarship.law.georgetown.edu/facpub/2190

265. Solove DJ. INTRODUCTION: PRIVACY SELF-MANAGEMENT AND THE CONSENT DILEMMA. *Harv Law Rev*. 2013;126:1880. Accessed September 1, 2022. http://bobgellman.com/rg-docs/rg-FIPPShistory.pdf.

266. Trade Regulation Rule on Commercial Surveillance and Data Security. Federal Register. Published August 22, 2022. Accessed August 28, 2022. https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

267. CISCO Cybersecurity Series. *Consumer Privacy Survey*.; 2019. Accessed August 9, 2021. https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/cybersecurity-series-2019-cps.pdf

268. Smith HJ, Milberg SJ, Burke SJ. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly*. 1996;20(2):167. doi:10.2307/249477

269. Graeff TR, Harmon S. Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*.

2002;19(4):302-318. doi:10.1108/07363760210433627

270. Culnan MJ. "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use. *MIS Quarterly*. 1993;17(3):341. doi:10.2307/249775

271. Kezer M, Sevi B, Cemalcilar Z, Baruh L. Age differences in privacy attitudes, literacy and privacy management on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*. 2016;10(1). doi:10.5817/CP2016-1-2

272. Patel V, Beckjord E, Moser RP, Hughes P, Hesse BW. The Role of Health Care Experience and Consumer Information Efficacy in Shaping Privacy and Security Perceptions of Medical Records: National Consumer Survey Results. *JMIR Med Inform 2015;3(2):e14 https://medinform.jmir.org/2015/2/e14*. 2015;3(2):e3238. doi:10.2196/MEDINFORM.3238

273. Norberg PA, Horne DR, Horne DA. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*. 2007;41(1):100-126. doi:10.1111/J.1745-6606.2006.00070.X

274. Norberg PA, Horne DR. Privacy attitudes and privacy-related behavior. *Psychol Mark*. 2007;24(10):829-847. doi:10.1002/MAR.20186

275. Barth S, de Jong MDT. The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*. 2017;34(7):1038-1058. doi:10.1016/j.tele.2017.04.013

276. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Comput Secur*. 2017;64:122-134. doi:10.1016/J.COSE.2015.07.002

277. Kelley PG, Cesca L, Bresee J, Cranor LF. Standardizing privacy notices. In: *Proceedings of the 28th International Conference on Human Factors in Computing Systems - CHI '10*. ACM Press; 2010:1573. doi:10.1145/1753326.1753561

278. Kröger JL, Lutz OHM, Ullrich S. The myth of individual control: Mapping the limitations of privacy self-management. *SSRN Electronic Journal*. Published online 2021. doi:10.2139/ssrn.3881776

279. Larson B, Belmas G. Second Class for the Second Time: How the Commercial Speech Doctrine Stigmatizes Commercial Use of Aggregated Public Records. *S C Law Rev*. 2007;58(4):935-994. Accessed September 4, 2022. https://scholarship.law.tamu.edu/facscholar/827

280. Ienca M, Ferretti A, Hurst S, Puhan M, Lovis C, Vayena E. Considerations for ethics review of big data health research: A scoping review. *PLoS One*. 2018;13(10):e0204937. doi:10.1371/JOURNAL.PONE.0204937

281. Garrison NA. Genomic Justice for Native Americans: Impact of the

Havasupai Case on Genetic Research. *Sci Technol Human Values*. 2013;38(2):201. doi:10.1177/0162243912470009

282. Reilly M. Is Facebook Targeting Ads at Sad Teens? | MIT Technology Review. MIT Technology Review. Published May 1, 2017. Accessed August 11, 2022. https://www.technologyreview.com/2017/05/01/105987/is-facebook-targeting-ads-at-sad-teens/

283. Barocas S, Nissenbaum H. Big data's end run around procedural privacy protections. *Commun ACM*. 2014;57(11):31-33. doi:10.1145/2668897

284. Kleiman J. Love Canal: A Brief History . SUNY Geneseo. Accessed April 14, 2022. https://www.geneseo.edu/history/love_canal_history

285. Dobkin A. Information Fiduciaries in Practice. *Berkeley Technol Law J*. 2018;33(1):1-52. Accessed August 29, 2022. https://www.jstor.org/stable/pdf/26490153.pdf

286. Barrett L. Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries. *Seattle University Law Review* . 2019;42:1057. Accessed March 9, 2020. https://perma.cc/WD94-ZRH8].

287. Kho ME, Duffett M, Willison DJ, Cook DJ, Brouwers MC. Written informed consent and selection bias in observational studies using medical records: systematic review. *BMJ*. 2009;338(7698):822. doi:10.1136/BMJ.B866

288. Emam K el, Jonker E, Moher E, Arbuckle L. A Review of Evidence on Consent Bias in Research. *The American Journal of Bioethics*. 2013;13(4):42-44. doi:10.1080/15265161.2013.767958

289. Council for International Organizations of Medical Sciences. INTERNATIONAL GUIDELINES FOR ETHICAL REVIEW OF EPIDEMIOLOGICAL STUDIES. *The Journal of Law, Medicine & Ethics*. 1991;19(3-4):247-258. doi:10.1111/j.1748-720X.1991.tb01822.x

290. Copeland R. Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans. Wall Street Journal. Published 2019. Accessed September 30, 2021. https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

291. Schmit CD. The tricky ethics of Google's Project Nightingale, an effort to learn from millions of health records. The Conversation. Published 2019. Accessed February 12, 2020. https://theconversation.com/the-tricky-ethics-of-googles-project-nightingale-an-effort-to-learn-from-millions-of-health-records-127219