AI Ethics, Law, and Policy

Pauline T. Kim

1. Introduction

Advances in artificial intelligence offer the potential for enormous societal benefit, but also raise risks of significant physical, economic and social harms. As a result, these technologies pose a challenge: how to channel their development to benefit society as a whole, while avoiding their harmful consequences. As AI is more widely incorporated into everyday systems, it poses increasing risks, including unfair or discriminatory treatment and threats to human health and safety. Growing awareness of these risks has in turn generated myriad efforts by private industry, academia, government agencies, legislators, and civil society groups to identify and mitigate potential harms of AI.

This chapter explores efforts to guide developments in AI in socially beneficial ways, examining the relevance of ethics, law and policy. *Ethics* focus on articulating important values and principles and are intended to guide behavior. Initiatives in this area identify principles to govern the development and use of AI tools, but typically lack any enforcement mechanism. *Laws* are enacted through some kind of public process and have binding effect. Actors who violate legal standards or requirements can face liability resulting in payment of damages or other penalties. *Policy-making* sometimes results in the passage of laws, but often has a broader, more exploratory emphasis, incorporating research, planning, and experimentation in an effort to identify solutions. The categories of ethics, law, and policy overlap and interrelate in important ways, but analyzing them as distinct categories helps to highlight the differences between them, as well as the advantages and limitations of each approach.

Efforts to ensure that AI works for societal benefit face several fundamental challenges. First, AI is notoriously difficult to define. Systems that autonomously replicate some form of human behavior are everywhere, ranging from trivial processing that follows clearly defined steps to highly complex systems that "learn" decision rules rather than having them specified by programmers in advance. As a result, the scope of the inquiry is ambiguous, making it hard to definitively enumerate all of the potential challenges raised by AI. Second, even if a definitive taxonomy of the issues could be developed, it would only be a first step. What is ultimately required is the creation of systems, structures, and laws that can effectively channel the development of AI to promote socially beneficial uses and mitigate the risks of harm.

A third challenge, closely related to the first two, is finding the appropriate level of generality for action given that AI refers to many different technologies and is used in many different contexts. A broad approach has the advantage of addressing the issues wholesale, but risks being either so vague as to be meaningless or so specific that it produces unintended consequences in atypical situations. An alternative strategy would create rules or guidelines for each specific context. While this approach is more precisely tailored, it is slower and more cumbersome to develop, and could leave significant gaps in coverage. The dilemma echoes a longstanding debate in the privacy literature regarding whether omnibus legislation or sector-specific regulation is preferable. [34,38]

Given these challenges, there is no single solution for guiding the development of AI. Instead, harnessing the benefits and avoiding the harms of AI will require a mix of approaches. This chapter explores the advantages and limitations of relying on ethical principles, legal rules, and policy-making to achieve these goals. To ground the discussion, it relies on a handful of commonly mentioned areas of concern as examples—namely, consumer privacy, bias and discrimination, and fairness in criminal law enforcement. Other concerns surrounding AI, such as environmental degradation, security breaches, and threats to health and safety, are also salient, and efforts to mitigate these harms could be subject to similar analyses of the interplay between ethics, law, and policy.

2. Ethical Principles

As awareness has grown that AI can cause harm, efforts to identify the ethical principles that should govern development of these systems have proliferated. Private firms, industry groups, government entities, intergovernmental organizations, and civil society groups have all undertaken initiatives in this area. In 2020, Fjeld et al. collected 36 prominent statements of ethical AI principles. [13] Similarly, Jobin et al. conducted a global survey and identified 84 such documents [19], while Schiff et al. evaluated 112 statements. [36] A crowdsourced list on AlgorithmWatch listed over 160 as of September 2022. [1]

Several studies have conducted meta-analyses of ethical AI principles to identify themes and look for areas of convergence or consensus. [5,16,41] Fjeld et al. [13] found eight prominent themes: privacy, accountability, safety and security, transparency and explainability, fairness and nondiscrimination, human control, professional responsibility, and promotion of human values. These themes are mentioned in nearly all of the documents they examined, and each in turn encompasses a number of subsidiary principles, resulting in a total of forty-seven identified principles. Jobin et al. [19] undertook a similar type of analysis on a larger sample of documents and concluded that there is an emerging global convergence around five core principles: transparency, justice and fairness, non-malfeasance, responsibility, and privacy. Schiff et al. [36] identified 25 topics, with the most prominent being social responsibility, transparency, bias and fairness, privacy, and safety and reliability.

AI principles are typically stated at a high level of generality. For example, protection of privacy appears in a majority of statements, but what exactly that entails is rarely explained. The Asilomar Principles of AI [14] address privacy in two sentences: "People should have the right to access, manage and control the data they generate" and "The application of AI to personal data must not unreasonably curtail people's real or perceived liberty." The OECD's discussion of privacy [29] is even briefer, including "privacy and data protection" in a list of human rights and democratic values that should be respected. Guidelines by the High-Level Expert Group on Artificial Intelligence (HLEG Guidelines) set up by the European Commission [12] say a bit more, explaining that protecting privacy "necessitates adequate data governance that covers the quality and integrity of data used, its relevance in light of the domain in which the AI systems will be deployed, its access protocols and the capability to process data in a manner that protects privacy."

While this added detail directs attention to aspects of the development process, it remains unclear how to operationalize the principle in a concrete setting.

Ethical principles that address risks of bias and discrimination are similarly vague. The OECD calls for "reducing economic, social, gender and other inequalities" and respecting democratic values including "non-discrimination and equality, diversity, fairness, [and] social justice." [29] The HLEG Guidelines state that AI systems should ensure "equal access through inclusive design processes, as well as equal treatment," that "identifiable and discriminatory bias should be removed" when collecting data, and that "oversight processes" should be put in place. [12] Other statements more vaguely refer to cultural diversity and human dignity, rights, and freedoms as important values. [14,18]

The articulation of ethical principles for AI is an important first step in moving away from technological determinism. These efforts entail recognition that AI systems are not technical artifacts with independent existence, but instead are part of sociotechnical systems. [32] The types of AI that are developed and the uses to which they are put are not inevitable; rather, their creation and deployment result from and reflect social processes, and their use will have profound societal consequences. AI principles can serve as a crucial acknowledgement and a reminder of these facts.

At the same time, ethical principles will likely have limited practical impact. They are inherently vague because they aim to guide behavior in a wide range of situations. Their generality offers the advantage of being broadly applicable, as well as increasing the likelihood that they will be widely endorsed. The downside to this breadth is that these principles often amount to little more than platitudes that do not grapple seriously with difficult ethical questions. No one would disagree that "justice and fairness" are desirable goals, but what does that mean when designing a system that will influence or determine who is released from jail or gets a job? Precisely because there is widespread disagreement about what justice requires in concrete settings, general principles will rarely help with difficult choices in the design or deployment of AI tools.

Consider the ethical principle of protecting personal privacy. What constraints does that principle put on the collection and analysis of information about individual people? AI systems that are used to screen and select people for employment, housing or credit rely on large amounts of personal data. Does protecting privacy entail limits on the types of personal information that can be collected? Or is it sufficient that individuals have consented to the collection of that information? Can their consent be presumed because they failed to opt out of a default setting? Does it matter whether they were told what information would be collected, how it would be used and what the potential social, financial, and reputational risks might be? In other words, do the conditions under which that consent was obtained matter? And once data has been collected, can it be used for any purpose, including making inferences about people? What if those inferences might reveal sensitive information such as a person's medical conditions, religious practices, or sexual preferences? These issues have been widely debated, but generalized statements about respecting individual privacy provide no clear answers, leaving practitioners free to interpret and apply the principles for themselves.

General statements of ethics may also mask significant underlying disagreements about the meaning of the articulated values. AI principles almost always include fairness and nondiscrimination, and yet the meaning of those terms is deeply contested. Invidious prejudice is easy to condemn, but beyond that baseline, the consensus around what is wrongful discrimination breaks down. On one view, unfair discrimination occurs only when a negative decision, such as refusing someone a job or denying them a loan, is based on a protected characteristic. So long as race or gender was not part of the decision, the demands of fairness of satisfied. Alternative views condemn decisions that systematically disadvantage groups that have been historically subordinated, such as people of color and women, regardless of whether it can be proven that the effects are intentional. Fairness would thus require more than avoiding intentional discrimination; it would also encompass a duty to avoid or dismantle systems that reinforce systemic inequality.

These debates mean that ethical principles of nondiscrimination are indeterminate when applied to AI systems. Fairness might turn on the inputs to a system, such that a model that does not include features like race or gender (and perhaps proxies for those characteristics as well) would be considered fair. Alternatively, fairness might require scrutiny of the outputs—specifically, whether the predictions of an AI system are fair across groups. Examining outputs leads to further questions about how to measure fairness—whether by requiring equal accuracy rates, equal false positive or false negative rates, equal outcomes, or something else. [25] Multiple formal measures of group fairness have been proposed in the computer science literature and it will often be impossible to satisfy them all. [25] Because statements of ethical AI do not resolve these debates, they cannot meaningfully constrain how the technology will be developed and deployed.

Ethical guidelines can also obscure ways in which high-level principles may conflict with one another and thereby avoid resolving those tensions. These guidelines often identify both protecting privacy and freedom from discrimination as important governing principles, but with little acknowledgement that the two values are sometimes in tension. One of the reasons predictive AI may exhibit bias is a lack of sufficient data for certain subgroups. As a result, efforts to reduce that bias will often motivate increased data gathering, which can in turn incentivize increased surveillance of disadvantaged and marginalized groups. And, depending upon the uses to which the technology is put, more accurate, less biased forms of AI could cause disproportionate harm to those communities. [15]

A case in point is facial recognition systems. After researchers [3] documented that several commercially available facial recognition systems made more errors on faces with darker skin tone, Microsoft responded by expanding the training and benchmark datasets and “launched new data collection efforts” in order to increase the accuracy of its tool “across all skin tones.” [35] In other words, it increased collection of images from communities of color. While Microsoft viewed these steps as positive efforts to reduce unequal accuracy rates, the impact on those communities is more ambiguous. Efforts to reduce bias and improving accuracy of facial recognition technologies stand in considerable tension with protecting personal privacy. If those technologies are then deployed disproportionately in communities of color by law enforcement, then the push to reduce bias also conflicts with their interests in reducing discriminatory policing.

Critics have argued that ethical guidelines are likely to have little actual effect. In one study [28], researchers instructed some software developers and students about ethical guidelines, then examined their responses to scenarios presenting ethical dilemmas. They found no differences in the responses of those who had received information about the ethical guidelines and those who had not. [28] In real world settings, where professionals face competitive pressures to create products and scale them quickly, it is even less likely that unenforceable guidelines will meaningful shape behavior, especially when ethical consideration conflict with immediate professional gains.

Observers have expressed particular skepticism about AI principles published by companies that build and profit from these technologies. [5,16] They argue that these statements are self-serving, encouraging the public to trust their AI, while providing no transparency as to how these systems work and little accountability for their consequences. By prominently announcing their commitment to ethics, these companies may be engaging in a form of "ethics-washing." These statements may signal concern about ethics in order to deflect public or government scrutiny and to forestall meaningful legal regulation while providing no real protection to the public. Consistent with these concerns, Schiff et al. [36] found that ethical statements from the private sector have less breadth and depth, and less engagement with law and regulation than statements from the public sector or non-governmental organizations.

A further criticism of ethical AI principles is that they tend to assume that the solutions are purely technical in nature rather than examining the broader social context. Statements by private entities are particularly prone to emphasize technical fixes to ethical challenges. [36] Greene et al. argue that many of these statements "co-opt the language of . . . critics, folding them into a limited, technologically deterministic, expert-driven view of what ethical AI/ML means." [15] For example, ITI's Global AI Policy Recommendation emphasizes the use of techniques such as anonymization, pseudonymization, de-identification, and other privacy enhancing techniques "to ensure data can be used to train algorithms and perform AI tasks without breaching privacy." [18] This recommendation emphasizes expert-driven responses to what are in fact contested social and political questions. It assumes individual privacy interests are only about non-disclosure, thereby narrowing the ethical inquiry to technologically-achievable solutions, rather than engaging a broader conversation about whether businesses and government should be permitted to collect all manner of personal data and what limits should be placed on how they use the data they do collect.

On the other hand, guidelines and principles can serve as useful tools for internal governance, shaping an organization's culture and values and channeling behavior of its agents toward socially appropriate goals. Their effectiveness, however, depends largely upon how they are implemented and whether the organization backs its broad principles with oversight and accountability mechanisms. Because ethical statements by private firms are typically intended to shape their internal culture or to communicate their values to the public, readers should understand them in light of those limited purposes. Private ethical statements are not universal principles identifying all relevant ethical concerns, nor should they be understood to delimit the appropriate sphere of regulation or public policy.

Standing alone, then, ethical principles will have quite limited impact. Not only are they vague and therefore difficult to operationalize, but the guidance they offer is not enforceable. They serve as aspirational goals rather than rules with binding effect.

3. Law

Unlike statements of ethical principles, legal rules have binding force. Laws are enacted through some type of public process, and they are backed by the power of the state or other governing entity. And while ethical principles are stated in aspirational terms—for example, the statement that AI applications should be “fair, transparent and accountable” [31]—legal rules are typically framed in terms of prohibitions. Laws prohibit employers or lenders from discriminating, forbid police from conducting certain searches without probable cause, bar health care providers from revealing personal medical information, and so on. These prohibitions are backed by sanctions of various sorts. An entity that violates a legal rule may face a lawsuit or an investigation by a regulatory agency. If a violation is found, it may be required to compensate another party for the harm, pay a penalty, or face a court order requiring compliance.

While the law operates with greater force than ethical principles, it also has significant limitations in shaping the development of socially beneficial AI. To start, a significant gap exists between what is lawful and what is ethical and socially responsible. Activities that produce significant harms and are socially undesirable may nevertheless be legally permissible. Thus, the fact that a firm is fully in compliance with existing law does not answer the question whether its activities are ethical and offers no guarantee that the technology it develops is socially beneficial.

A gap between law and ethics can occur for a number of reasons, but it is often due to lags in regulation. New technologies and practices are constantly introduced, but the risks and harms they pose are not immediately apparent. Once problems are identified, it takes time to sort out how existing laws apply and whether they are sufficient to address those harms. Where existing law does not adequately address the risks of harm, new legislation may be needed to fill the gaps. Drafting new laws, however, can be challenging. With complex and evolving technologies, it is difficult to craft clear legal rules delineating what is permissible and what is not. Moreover, legislators often lack technical expertise and may be highly influenced by industry lobbyists seeking to avoid regulation. As a result, lawmakers may fail to adequately take into account the interests of a diffuse, unorganized public, or marginalized groups like criminal defendants or low-income workers who may be negatively impacted by AI applications.

Concerns about the potential for discrimination and invasions of privacy illustrate these challenges. Regarding discrimination, existing laws provide a framework for challenging discriminatory AI; however, some gaps and uncertainties remain because the laws were enacted with human decision-makers in mind. In the case of threats to privacy, technological developments have largely outstripped prior legal approaches, leaving significant gaps in protection, particularly under U.S. laws.

Traditional legal doctrine recognizes two distinct theories of discrimination: disparate treatment and disparate impact. Disparate treatment involves adverse treatment of an individual *because of* a protected characteristic like race, sex, or disability. When dealing with human decision-makers, courts typically frame that causal inquiry as a question of intentional discrimination—i.e. was the decision-maker motivated by the protected characteristic. [44] Disparate impact cases do not require proof of intent, but instead focus on discriminatory effects. [43] Liability for disparate impact discrimination arises when a facially neutral procedure or practice disproportionately harms a protected group and no legitimate business reason justifies that practice.

The analysis of a disparate impact case under U.S. law generally proceeds in three steps. First, a party challenging a particular practice as discriminatory must show that it has a "disparate impact," typically by producing statistical evidence that the practice disproportionately screens out members of a disadvantaged group. Next, the decision-maker has the opportunity to show that its selection procedure is justified by business reasons in order to escape liability. Even if it does so, in the final step, the party challenging the practice can nevertheless prevail by showing the existence of a less discriminatory alternative that would meet the decision-maker's legitimate needs but that it failed to adopt. [46]

The most common use of the disparate impact theory has been to challenge employment tests and requirements. The Supreme Court case that first recognized the theory is *Griggs v. Duke Power Co.* [43] A group of Black workers sued Duke Power Company, challenging its policy that a high school diploma and minimum scores on a standardized test were required for certain skilled positions. These requirements had the effect of barring far more Black than white workers from the higher-paying jobs because a long history of segregated schools in the region had deprived them of equal educational opportunities. Because the requirements bore no relationship to the skills needed to successfully perform the jobs at issue, the Court found that imposing these requirements was discriminatory and violated federal anti-discrimination law. Subsequent cases have involved challenges to other written tests, or requirements like minimum height and weight requirements that disproportionately screen out female applicants. [46,48]

How do these legal theories of discrimination apply to AI tools? Consider first the theory of disparate treatment. If the creator of an AI tool deliberately designs it with the *purpose* of screening out members of a historically disadvantaged group, that effort would clearly amount to disparate treatment discrimination. Proof of motive might be challenging, but this scenario presents no particular conceptual difficulty. On the other hand, the mere fact that the creators of a predictive tool did not intend to discriminate is not decisive of the legal question. In complex machine learning models, close proxies often exist for characteristics like race and sex, and predictive models can incorporate human biases or reproduce existing patterns of disadvantage or exclusion. [2] When this happens, an AI tool may systematically disadvantage historically subordinated groups, such as racial minorities or women. [23]

In situations like these, disparate impact theory will prohibit practices that have unjustified discriminatory effects. However, ambiguity exists as to how existing doctrine should be applied to predictive AI tools. For example, under the second step of the analysis, employers can defend against a disparate impact claim by showing its requirements are "job related for the position in question and consistent with business necessity." [58] With a traditional employment test, an employer does so by demonstrating its validity—i.e. by showing that the test or requirement actually measures job-relevant skills or attributes. [49] This concept of job validation is rooted in the industrial psychology literature and focuses on measuring individual skills and capacities.

AI tools, however, typically do not start with an analysis of the skills needed to do a job, but instead extract patterns from the available data to predict candidates' future performance. The data used to train the model may contain features that are strongly predictive of the target variable, yet have no clear connection to job performance. Given the complexity and opacity of some ML models, an employer may not be able to explain how a decision to hire or reject a specific candidate was reached. Uncertainty about how to apply the concept of job validation leaves room for companies to argue that so long as they can demonstrate a statistical correlation with the outcome of interest, an AI screening tool should not be considered discriminatory, even if it produces a disparate impact.

The problem with this approach is that it fails to recognize that a robust statistical correlation may mask reliance on factors that are wholly arbitrary or implicitly discriminatory. Data mining often uncovers unexpected or even inexplicable correlations, not all of which are fair to rely on. One study found that liking curly fries on Facebook was correlated with higher intelligence. [26] Clearly, the relationship is not causal, nor is there any direct or necessary relationship between the two variables, apart from their coincidence in the particular dataset studied. But suppose an employer relied on a strong correlation between liking something on Facebook and positive job performance to justify a selection tool that had a discriminatory effect. No court would accept this justification, because such a tool would create "'built-in headwinds' for minority groups" and be "unrelated to measuring job capability," which is exactly the type of practice condemned by the Supreme Court in the *Griggs* case. [43]

Alternatively, an algorithm might capture real differences between groups, but in ways that leverage proxies for protected characteristics. For example, a hiring algorithm that aims to predict longevity on the job may systematically screen out or disfavor women of childbearing age and individuals with disabilities because they are statistically more likely to take breaks from employment. If an employer explicitly relied on childbearing capacity or disability to screen applicants, it would violate the law. The legal outcome should not be different when an opaque model produces the same effects.

If AI tools could be justified based on a strong statistical correlation alone, they could in effect deprive people of opportunities based on proxies for protected characteristics or wholly arbitrary features. A better application of disparate impact theory would require an employer to demonstrate the *substantive validity* of its selection tools. [23] The mere existence of a statistical correlation should not be sufficient to justify a model with discriminatory effects. Instead, the employer should bear the burden of showing that the model was built using accurate, representative, and unbiased data, and that it actually measures job-relevant skills and abilities. A coalition of prominent civil rights organizations endorsed such an approach, stating that "organizations should do the necessary work of studying and understanding the knowledge, skills, and abilities required by a particular job," and that "mere correlations between traits and purported job performance should not be sufficient to justify adverse impact." [39]

Because predictive models can produce discriminatory effects, government agencies, employers, banks, and other entities that use these tools should regularly audit their performance. If they find unwarranted discriminatory effects, they have a legal responsibility to correct the problem or stop using the tool. However, efforts to correct a discriminatory algorithm may raise further legal questions. Some researchers have asked whether efforts to *remove* discriminatory effects might themselves run afoul of anti-discrimination law by taking account of race, sex, or other protected characteristics. [24] In other words, they question whether considering sensitive characteristics in an effort to debias algorithms amounts to disparate treatment discrimination.

Although the courts have not addressed this issue in the context of AI tools, several legal principles emerge from past cases. First, employers and other entities are permitted to *prospectively* change practices that they discover have an unjustified disparate impact. Apart from the rare circumstance in which applicants have relied to their detriment on a previously announced policy, by, for example, expending time and money to study for a specific test [57], an employer is free to adjust its selection procedures going forward. [60,59] In fact, the Supreme Court has repeatedly emphasized the importance of voluntary employer efforts to remove discriminatory practices, stating that voluntary compliance is the "preferred means" and "essential" to achieving the objectives of anti-discrimination law. [50,51]

Past cases have also permitted taking race and other sensitive characteristics into account in order to ensure equal access to opportunities. For example, courts have permitted employers to take affirmative steps to recruit more women and racial minorities to build a broad and diverse applicant pool. [53–55] Courts have also viewed with favor efforts to obtain data from underrepresented groups to avoid inadvertently creating biased tests. [57] These opinions suggest that efforts made when building a model to prevent discriminatory outcomes pose no particular legal problems. [24] Designers can examine proposed target variables for implicit bias and select a target that avoids that problem. They can scrutinize the representativeness and accuracy of training data, oversample underrepresented groups, or remove features that encode human bias, such as subjectively coded attributes. While these types of strategies pay attention to race or other sensitive characteristics in order to build selection processes that are fair to all, they do not make decisions about individuals turn on those characteristics.

More difficult is the question whether race or other protected characteristics can *explicitly* be taken into account as a feature in order to reduce bias against historically disadvantaged groups. On the one hand, models that simply ensure a fixed proportion of positive outcomes across population subgroups regardless of the distribution of other characteristics is likely unlawful. Courts have repeatedly criticized rigid numerical goals and found race and gender quotas impermissible.

On the other hand, sensitive characteristics might be incorporated in other ways that arguably make a model fairer. If, for example, greater uncertainty surrounds the estimates for a sub-population, or a predictive feature interacts with characteristics like race or sex in distinct ways, then including the sensitive characteristic in the model may make it more accurate across demographic groups. [9,10] In such cases, strong arguments exist that taking these characteristics into account are not discriminatory, either in intent or effect. [24] How courts would view such arguments, however, is uncertain.

Although some areas of ambiguity exist, current anti-discrimination law offers a useful conceptual framework for analyzing and challenging biased AI tools. However, practical obstacles also make addressing discriminatory harms difficult. Anti-discrimination laws are primarily enforced when individuals bring lawsuits alleging they have suffered harm from a discriminatory decision.[1] This enforcement mechanism is less effective in a world in which decisions are rendered on a mass scale by complex algorithms operating behind the scenes. Individuals cannot easily detect when and how they have been affected by potentially discriminatory decisions. For that reason, many researchers have called for entities to give clear notice when relying on automated decision systems and to provide greater transparency about how those systems operate. [6]

Those calls have in turn generated debate over what meaningful notice and transparency require. [11,20,22,40,17] Some have asserted that individuals subject to AI screening tools should have a right to an explanation for an adverse decision, a right to contest the decision, or a right to human review. Even with these rights, however, it will be difficult for an individual to challenge a systemically biased model. Doing so will require data showing how the system as a whole operates, not just in the individual case. It will also require significant resources and a high level of technical expertise unlikely to be available to an individual litigant. These practical obstacles to enforcing legal liability rules have led many to consider broader regulatory and policy approaches to prevent discrimination, as discussed in part 4 below.

In contrast to anti-discrimination law, which offers some leverage for challenging AI tools, privacy law in the U.S. has been outstripped by technological developments. Two aspects in particular make it unsuited to protecting personal information in an era of big data and artificial intelligence. First, U.S. law has taken a sectoral approach, focusing on certain types of highly sensitive information, leaving gaps in coverage as data collection and use has expanded. [34] Second, the law relies heavily on notice and consent to govern data privacy, which has permitted business and government to amass enormous amounts of personal information. [37]

Unlike Europe, which takes an omnibus approach to data protection, [61] U.S. law is fractured depending upon the type of information at issue. For example, certain federal laws restrict who can gather medical and genetic information about specific individuals. [52,56] Another law prohibits disclosure of educational records [45], and yet another regulates consumer records. [42] The common law tort of invasion of privacy, which appears to apply broadly, is also limited in scope. Because the privacy tort aims to redress intrusions that are "highly offensive to a reasonable person," [47] it focuses on inquiries or exposures that are embarrassing or humiliating, for example, involving medical conditions or sexual practices. The assumption underlying much existing legal protections for privacy in the U.S. is that certain types of information are particularly sensitive and warrant special protection. Other information that is viewed as non-sensitive or trivial can be collected with few restrictions.

At the same time, U.S. law has viewed privacy primarily as a matter of personal control over information, and therefore has leaned heavily on a regime of notice and consent. [37] Laws give people rights to know about and review information collected about them, and rights to agree to or refuse collection of their personal information. With this set of tools, they are expected to engage in "privacy self-management"—i.e. to protect their own interests by exercising their rights to access their data records or to withhold consent to their collection in the first place. [37] This emphasis on consent has legitimated the collection and use of all manner of personal data, on the assumption that people are capable of protecting their own interests.

[1] Anti-discrimination law can also be enforced by government agencies, but those cases today represent only a very small fraction of discrimination lawsuits.

The growth of AI technologies has put increasing strain on this framework, rendering it largely ineffective in protecting personal information. To start, the need for large datasets to train AI tools has created enormous demand for increasingly comprehensive information about more people. At the same time, the explosion of available data and rapid advances in computing power have rendered the assumptions underlying traditional privacy protections increasingly obsolete. The distinction between "sensitive" and "non-sensitive" personal information is becoming meaningless. Small bits of information about individuals, such as their consumer purchases, may seem quite trivial when viewed in isolation, and therefore, not to warrant protection. However, AI can aggregate those data points across time and populations, then mine them for new insights, revealing highly sensitive information, such as sexual orientation, medical risks or conditions, or whether someone is pregnant. Because entities with large amounts of data can "derive the intimate from the available," [4] prohibiting them from collecting "sensitive" data will not prevent them from inferring that same information. As a result, regulation solely at the sectoral level leaves large gaps in coverage.

For similar reasons, relying on consent to protect personal information is increasingly problematic in a world of big data and machine learning. [33,37] Privacy disclosures are notoriously long, complex, and difficult to understand. No one has the time or cognitive bandwidth to read and comprehend all of the privacy policies encountered in daily life in order to exercise meaningful choice about what information to share. Even if it were possible, many policies are non-negotiable, and people cannot realistically refuse the collection and use of their personal information when doing so is a condition of accessing essential services.

AI tools put pressure on the notice and consent regime in another way as well. Because AI can produce novel insights from existing data, or leverage information in wholly unanticipated ways, it is impossible for people to rationally weigh the costs and benefits of sharing their personal data. The downstream uses of that information and the potential impact on their interests are unknowable at the time they are asked to consent to its collection. The solution is not simply to provide better notice in the form of more information. The entity collecting the information cannot anticipate all possible future uses, especially if the data may be shared or combined with other datasets. And adding more detailed, technical, and contingent information to privacy disclosures would only increase information overload and further vitiate meaningful consent.

Insights derived from AI may render consent altogether irrelevant in some contexts. As computational tools have become more powerful, it is no longer necessary to collect information from a particular person in order to learn about that individual. Data collected from *other* people can reveal startling insights, as demonstrated by the use of genetic databases to identify murder suspects, even though the suspects themselves had never shared their genetic data. Thus, advances in AI have largely rendered obsolete the traditional US approach of relying on sectoral regulation, and notice and consent, to protect personal information.

The European Union has taken a different approach. The General Data Protection Regulation (GDPR) [61], which became effective in 2018, addresses data protection in a number of ways quite distinct from U.S. law. It takes an omnibus approach, applying to all entities that process personally identifiable data, rather than limiting its focus to particular sectors or types of entities. The definition of data processors is broad, encompassing entities that handle personal data across multiple stages, from initial collectors to aggregators and brokers, to downstream users of the data. In addition, the GDPR imposes a more robust requirement of consent, rendering consent ineffective "where there is a clear imbalance between the data subject and the [data] controller." [61] In those situations, an entity may not rely on a thin conception of consent, but must instead justify its processing of personal data by some other means, such as by demonstrating that doing so is necessary to meet legitimate needs.

While the GDPR was primarily intended to update the EU's approach to regulating the collection and use of personal data, it also addresses the use of automated decision systems. The Regulation requires entities to inform individuals if they are subject to automated decision systems and a right to opt out of a decision based solely on automated processing "which produces legal effects . . . or similarly significantly affects him or her." [art. 22(1)] [61] Entities that use automated decision tools must also provide "meaningful information about the logic involved" [art. 14(2)(g)] and give individuals subject to those decisions the right "to obtain human intervention . . . and to contest the decision." [art. 22(3)] [61] While there is still uncertainty about how they apply, these provisions provide avenues for challenging the fairness of algorithmic decisions. Through its proposed Regulation on Artificial Intelligence, which complements the data protection regime of the GDPR, the European Union is poised to create a more comprehensive framework aimed at promoting beneficial uses of AI and mitigating its risks.

Recently, jurisdictions in the U.S. have begun to explore omnibus approaches to protecting personal data. Most notably, California enacted the first comprehensive state-level consumer privacy law, and was soon followed by a handful of other states. [62–67] These laws have largely built on traditional data protection principles, emphasizing protections such as consumers' rights to know what data is collected, and to correct or request deletion of their personal information. However, some of these laws also appear to provide a right to opt out of automated decisions, similar to the GDPR, and legislation has been introduced in Congress that would create omnibus approaches to regulating data privacy and algorithmic decision-making. [7,8,30]

In sum, traditional forms of legal regulation offer both advantages and disadvantages for shaping the development of AI. Unlike ethical principles, legal rules are more likely to be concrete, specific, and enforceable. At the same time, however, law often lags significantly behind social and technological developments. As discussed above, anti-discrimination laws offer a basis for challenging some forms of unfairness in AI tools, but because they have been interpreted with human decision-makers in mind, uncertainty remains about exactly how they apply to machine learning algorithms. Traditional legal conceptions of privacy have proven more problematic, as advances in AI have rendered those protections for personal information largely obsolete.

The difficulties with relying on legal regulation, however, do not stem merely from time lags. Lawmaking requires clearly delineating what activities are permitted and which are forbidden, a daunting task given the complexity and rapidly evolving nature of AI. This challenge is heightened because the use cases for AI are pervasive throughout society and widely varied in application. What risks are tolerable, and how they should be weighed against potential benefits, will differ depending upon the context and the gravity of the harm threatened. Because of the limitations inherent in traditional forms of direct regulation, researchers and policymakers are increasingly turning to a broader array of policy tools to govern the development of AI.

4. Policy

Policy has a broader focus than traditional lawmaking, as it seeks to promote socially beneficial outcomes rather than redressing harms suffered by particular individuals. Legal liability regimes are typically backward looking, coming into play after harm has occurred and focusing on questions of causation, culpability, and compensation. In contrast, policy approaches are forward looking, emphasizing strategies to achieve broad societal goals such as preventing environmental degradation or improving population health outcomes. Policy is softer than law, leveraging a variety of tools in an effort to influence behavior toward the desired ends.

Law and policy are not mutually exclusive. Laws that impose liability for causing harm can be part of an overall policy strategy to discourage socially negative behavior. Conversely, many policy levers require legal action—for example, to provide public funds for research, to create incentives to pursue certain activities, or to establish government agencies with oversight powers. Despite the overlap between law and policy, it is useful to consider policy approaches as distinct from the traditional legal focus on retrospective liability.

Some of the reasons for turning to policy tools for governing the development of AI were suggested in the previous section. AI tools are technologically complex, and their inner workings are often opaque. Their complexity and the need for deep technical expertise to understand the risks and tradeoffs make it difficult for lawmakers to articulate clear rules delineating in advance precisely which uses are permissible and which are not. In addition, the black box nature of many AI systems makes questions of causation and responsibility, which are central to retrospective liability schemes, very difficult to resolve. Individuals who are harmed by AI technologies may lack access to the resources or the expert knowledge needed to effectively litigate these issues.

A further reason for turning to policy solutions is that an individual rights-based approach is inadequate for recognizing and addressing broad societal harms. Legal liability focuses on the impact of a particular activity on identifiable people, but some of the most troubling effects of AI are systemic in nature. For example, an individual discrimination lawsuit would turn on the specific reasons that a particular person was not hired or was denied a loan, overlooking problems that only appear in the aggregate. If predictive algorithms systematically and unjustifiably disadvantage certain demographic groups when distributing benefits or opportunities, those effects are unlikely to be visible from the perspective of an individual lawsuit. Similarly, privacy rights that focus on an individual's choice to share information miss the larger context in which the actions of countless other people and entities determine what is known about that person.

Because of the limitations of law as a solution, attention has increasingly turned to other forms of governance. The European Union's GDPR takes steps in this direction in addition to the individual rights mentioned in part 3 above, by, for example, requiring entities that process personal data to comply with record-keeping requirements [art. 30] and to conduct impact assessments [art. 35] [61]. The Regulation also empowers public agencies to order disclosure of certain information about automated decision systems and to conduct audits. [art. 58(1)] [61] The

EU's Draft Artificial Intelligence Act goes further in this direction, requiring "high-risk" AI systems (systems that pose high risk to the health and safety or fundamental rights of natural persons) to undergo pre-market registration and assessment, as well as an ongoing, iterative process of identifying, evaluating, reporting, and managing risks once deployed. [21] Proposed legislation in the US would empower a federal agency to create requirements that entities that use AI-powered decision tools must engage in testing, assessment and documentation of the impact of those systems. [8]

These legislative initiatives, as well as scholarly articles and policy papers, are promoting a wide array of policy strategies for governing the development of AI. They include proposals that AI tools be licensed, subject to design standards, or required to undergo pre-market testing and certification, either by a government agency or trusted third party. Alternatively, particularly with highly regulated applications, government agencies may create regulatory sandboxes which permit companies to experiment with new technologies in a supervised and controlled environment. Other approaches emphasize the importance of self-assessment, imposing a duty on entities to consider the societal impacts of automated decision-making, and to take into account their effects on health and safety, the environment, or fundamental human rights. Once a system has been deployed, companies might be required to audit its real-world effects or to comply with mandated forms of public disclosure or reporting.

It is beyond the scope of this chapter to fully explore and evaluate these various policy tools for governing the development of AI. More generally, though, policy approaches offer distinct advantages and disadvantages as compared with traditional legal liability regimes. On the plus side, policy tools can be more open-ended and experimental in nature, allowing for flexibility and nimbleness in responding to evolving technology. Government agencies can undertake research about the variety of uses of AI, the likely future development of these technologies, and the possible outcomes they will produce. In doing so, they might involve technical experts as well as affected members of the public, and thereby expand the range of stakeholders participating in developing policy beyond what is typical in the legislative process.

Policy levers can also be used to influence the development of AI *ex ante*—for example, by assuring conformity with technical standards or design principles for privacy and fairness. These strategies may be more effective than *ex post* efforts at regulation because it will be increasingly difficult to identify and remove problems after significant investments have been made in building complex systems. Finally, policy approaches offer the opportunity to widen the lens and view technological challenges in a broader social context. Doing so will expand the choice set of possible actions beyond narrowly technical solutions. For example, to the extent that AI substitutes for human labor, observers have raised alarms that it will cause massive unemployment. If these concerns are considered solely from a technical perspective, the alternatives seem quite stark—either ban or strictly restrict the development of AI, or accept massive unemployment and the resulting social dislocation it will likely cause. A broader policy perspective brings into view numerous related social policies, such as the level of investment in education and training, public provision of essential needs like health care and retirement income which are currently linked to employment, and other policies that shape how economic gains and wealth are distributed across the economy.

Policy tools have weaknesses as well, and relying on them will not ensure that AI is developed in socially beneficial ways. To a large extent, the effectiveness of policy initiatives will depend upon which strategies are chosen, and the details of how they are implemented. If the policy levers chosen rely too heavily on procedural requirements, such as conducting assessments and filing reports, they may incentivize empty compliance gestures at the expense of taking concrete steps to prevent harm. Similarly, a system premised on self-regulation by affected firms runs the risk of being toothless without clear standards by which to measure compliance and meaningful enforcement mechanisms. Giving government agencies power to promulgate and enforce appropriate regulations may be more effective; however, there remains a risk of regulatory capture, where actors from the regulated industry influence or even dominate the government agencies that are tasked with overseeing them.

Many current and proposed strategies for governing the development of AI rest on a model of risk regulation. That approach makes some sense given the reasons that AI systems pose risks: they are technologically complex, difficult to understand, and likely to fail, but in ways that are difficult to predict. On the other hand, a risk regulation model has inherent limitations when applied to AI. [21] Some of the harms threatened by AI, such as privacy intrusions and discrimination, do not fit easily into traditional risk models because they are difficult to measure or quantify, and their very meaning is contested. They are not purely technical challenges, but rather pose "hybrid technical-policy problems" that should be solved through public consideration and debate rather than by technical experts. [21] And while risk regulation tools can be useful in mitigating future harms, another significant limitation is that they typically lack a mechanism for compensating people who actually suffer harm.

Conclusion

AI technologies promise many benefits, but they can also have significant negative impacts on human health, safety, well-being, and fundamental rights. Ethical, legal, and policy approaches offer tools to address these concerns; however, each has limitations and none provides a complete solution in itself. Statements of ethical principles can articulate high-level values and goals to guide behavior, but are usually quite vague and difficult to operationalize. They also lack any enforcement mechanism. In contrast, legal rules are enforceable through court action, and offer a way to compensate those suffering actual harms. However, the complexity and opacity of AI poses challenges to legal liability regimes by making it difficult to parse questions of causation and culpability. In addition, legal rules may not keep up with the rapid evolution of AI technologies. Policy tools are more flexible and forward-looking, and can help to anticipate and prevent harms, but may be ineffective if they lack robust standards or fail to require meaningful accountability from those who develop and deploy AI tools. Because each strategy has strengths and limitations, preventing social harms from the application of AI will require leveraging all three types of tools in complementary ways.

References

[1] AlgorithmWatch. 2020. About. *AI Ethics Guidelines Global Inventory*. Retrieved September 15, 2022 from https://inventory.algorithmwatch.org/about

[2] Solon Barocas and Andrew D. Selbst. 2016. Big Data's Disparate Impact. *Calif. L. Rev.* 104, 3 (2016), 671–732.

[3] Joy Buolamwini and Timnit Gebru. 2018. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In *Conference on Fairness, Accountability and Transparency*, PMLR, 77–91.

[4] Ryan Calo. 2017. Artificial Intelligence Policy: A Primer and Roadmap. *U.C.Davis L. Rev.* 51, (2017), 300–435. DOI:https://doi.org/10.2139/ssrn.3015350

[5] Corinne Cath, Sandra Wachter, Brent Mittelstadt, Mariarosaria Taddeo, and Luciano Floridi. 2018. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Sci. Eng'g. Ethics* 24, 2 (2018), 505–528. DOI:https://doi.org/10.1007/s11948-017-9901-7

[6] Danielle Keats Citron and Frank Pasquale. 2014. The Scored Society: Due Process for Automated Predictions Essay. *Wash. L. Rev.* 89, 1 (2014), 1–34.

[7] Yvette D. Clarke. 2019. *Algorithmic Accountability Act of 2019*.

[8] Yvette D. Clarke. 2022. *Algorithmic Accountability Act of 2022*.

[9] Sam Corbett-Davies and Sharad Goel. 2018. The Measure and Mismeasure of Fairness: A Critical Review of Fair Machine Learning. *arXiv:1808.00023 [cs]* (August 2018). Retrieved March 17, 2021 from http://arxiv.org/abs/1808.00023

[10] Cynthia Dwork, Moritz Hardt, Toniann Pitassi, Omer Reingold, and Richard Zemel. 2012. Fairness through awareness. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference on - ITCS '12*, ACM Press, Cambridge, Massachusetts, 214–226. DOI:https://doi.org/10.1145/2090236.2090255

[11] Lilian Edwards and Michael Veale. 2017. Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking For. *Duke Law & Technology Review* 16, 1 (December 2017), 18–84.

[12] European Commission High-Level Expert Group on Artificial Intelligence. 2019. Ethics Guidelines for Trustworthy Artificial Intelligence. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[13] Jessica Fjeld, Nele Achten, Hannah Hilligoss, Adam Nagy, and Madhulika Srikumar. 2020. *Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-Based Approaches to Principles for AI*. Berkman Klein Center for Internet & Society. Retrieved July 26, 2022 from http://nrs.harvard.edu/urn-3:HUL.InstRepos:42160420

[14] Future of Life Institute. 2017. Asilomar AI Principles. *Future of Life Institute*. Retrieved August 5, 2022 from https://futureoflife.org/2017/08/11/ai-principles/

[15] Daniel Greene, Anna Lauren Hoffmann, and Luke Stark. 2019. Better, Nicer, Clearer, Fairer: A Critical Assessment of the Movement for Ethical Artificial Intelligence and Machine Learning. In *Hawaii International Conference on System Sciences 2019 (HICSS-52)*, Grand Wailea, Hawaii, 2122–2131.

[16] Thilo Hagendorff. 2020. The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds & Machines* 30, 1 (March 2020), 99–120. DOI:https://doi.org/10.1007/s11023-020-09517-8

[17] Aziz Z. Huq. 2020. A Right to a Human Decision. *Va. L. Rev.* 106, 3 (May 2020), 611–688.

[18] Information Technology Industry Council. ITI's Global AI Policy Recommendations. Retrieved August 3, 2022 from https://www.itic.org/documents/artificial-intelligence/ITI_GlobalAIPrinciples_032321_v3.pdf

[19] Anna Jobin, Marcello Ienca, and Effy Vayena. 2019. Artificial Intelligence: the global landscape of ethics guidelines. *Nat. Mach. Intell.* 1, 9 (2019), 389–399.

[20] Margot E. Kaminski. 2019. The Right to Explanation, Explained. *Berkeley Tech. L. J.* 34, (January 2019), 189–218. DOI:https://doi.org/10.15779/Z38TD9N83H

[21] Margot E. Kaminski. 2023. Regulating the Risks of AI. *B.U. L. Rev.* 103, (September 2023). DOI:https://doi.org/10.2139/ssrn.4195066

[22] Margot E. Kaminski and Jennifer M. Urban. The Right to Contest AI. *Colum. L. Rev.* 121, 7 , 1957–2048.

[23] Pauline T. Kim. 2017. Data-Driven Discrimination at Work. *William & Mary Law Review* 58, 3 (February 2017), 857.

[24] Pauline T. Kim. 2022. Race-Aware Algorithms: Fairness, Nondiscrimination and Affirmative Action. *Calif. L. Rev.* (January 2022).

[25] Jon Kleinberg, Sendhil Mullainathan, and Manish Raghavan. 2016. Inherent Trade-Offs in the Fair Determination of Risk Scores. *arXiv:1609.05807 [cs, stat]* (2016), 1–23.

[26] Michal Kosinski, David Stillwell, and Thore Graepel. 2013. Private traits and attributes are predictable from digital records of human behavior. *Proc Natl Acad Sci U S A* 110, 15 (April 2013), 5802–5805. DOI:https://doi.org/10.1073/pnas.1218772110

[27] Daniel McMillan and Barry Brown. 2019. Against Ethical AI. In *HTTF 2019*, 1–3. DOI:https://doi.org/10.1145/3363384.3363393

[28] Andrew McNamara, Justin Smith, and Emerson Murphy-Hill. 2018. Does ACM's code of ethics change ethical decision making in software development? In *ESEC/FSE 2018*, Lake Buena Vista, FL, 729–733. DOI:https://doi.org/10.1145/3236024.3264833

[29] Organisation for Economic Cooperation and Development. 2022. Recommendation of the Council Artificial Intelligence. Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

[30] Frank Pallone. 2021. *American Data Privacy and Protection Act*.

[31] Partnership on AI. Partnership on AI: Our Tenets. *Partnership on AI*. Retrieved August 5, 2022 from https://partnershiponai.org/about/#tenets

[32] Ibo van de Poel. 2020. Embedding Values in Artificial Intelligence (AI) Systems. *Minds and Machines* 30, (2020), 385–409. DOI:https://doi.org/10.1007/s11023-020-09537-4

[33] Neil M. Richards and Woodrow Hartzog. 2019. The Pathologies of Digital Consent. *Wash. U. L. Rev.* 96, 6 (2019), 1461–1503.

[34] Neil M. Richards, Andrew B. Serwin, and Tyler Blake. 2022. Understanding American Privacy. In *Research Handbook on Privacy and Data Protection Law: Values, Norms and Global Politics*. Edward Elgar Publ'g, 60–72.

[35] John Roach. 2018. Microsoft improves facial recognition to perform well across all skin tones. *The AI Blog*. Retrieved September 15, 2022 from https://blogs.microsoft.com/ai/gender-skin-tone-facial-recognition-improvement/

[36] Daniel Schiff, Jason Borenstein, Justin Biddle, and Kelly Laas. 2021. AI Ethics in the Public, Private, and NGO Sectors: A Review of a Global Document Collection. *IEEE Transactions on Tech. & Soc'y* 2, 1 (2021), 31–42. DOI:https://doi.org/10.1109/TTS.2021.3052127

[37] Daniel J. Solove. 2013. Privacy Self-Management and the Consent Dilemma. *Harv. L. Rev.* 126, (2013), 1880–1903.

[38] Daniel J. Solove. 2015. The Growing Problems with the Sectoral Approach to Privacy Law. *TeachPrivacy*. Retrieved September 19, 2022 from https://teachprivacy.com/problems-sectoral-approach-privacy-law/

[39] The Leadership Conference on Civil and Human Rights. 2020. *Civil Rights Principles for Hiring Assessment Technologies*. Retrieved September 28, 2022 from https://civilrights.org/resource/civil-rights-principles-for-hiring-assessment-technologies/

[40] Sandra Wachter, Brent Mittelstadt, and Luciano Floridi. 2017. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law* 7, 2 (May 2017), 76–99. DOI:https://doi.org/10.1093/idpl/ipx005

[41] Yi Zeng, Enmeng Lu, and Cunqing Huangfu. 2019. Linking Artificial Intelligence Principles. In *Proceedings of the AAAI Workshop on Artificial Intelligence Safety 2019*.

[42] 1970. *Fair Credit Reporting Act*.

[43] 1971. *Griggs v. Duke Power Co.*

[44] 1973. *McDonnell Douglas Corp. v. Green*.

[45] 1974. *Family Educational Rights and Privacy Act of 1974*.

[46] 1975. *Albemarle Paper Co. v. Moody*.

[47] 1977. The Restatement (Second) of Torts § 652B.

[48] 1977. *Dothard v. Rawlinson*.

[49] 1978. Uniform Guidelines on Employee Selection Procedures. *29 C.F.R. § 1607*. Retrieved September 27, 2022 from https://www.ecfr.gov/current/title-29/subtitle-B/chapter-XIV/part-1607

[50] 1986. *Wygant v. Jackson Bd. of Educ.*

[51] 1986. *Local No. 93, Intern. Ass'n of Firefighters, AFL-CIO C.L.C. v. City of Cleveland*.

[52] 1996. *Health Insurance Portability and Accountability Act of 1996*.

[53] 1997. *Duffy v. Wolle*.

[54] 2005. *Rudin v. Lincoln Land Community College*.

[55] 2006. *Mlynczak v. Bodman*.

[56] 2008. *Genetic Information Nondiscrimination Act of 2008*.

[57] 2009. *Ricci v. DeStefano*.

[58] 2010. *42 U.S.C. § 2000e-2*.

[59] 2010. *Carroll v. City of Mount Vernon*.

[60] 2013. *Maraschiello v. City of Buffalo Police Dept.*

[61] 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016 OJ (L 119).

[62] 2018. *California Consumer Privacy Act of 2018*.

[63] 2020. *California Privacy Rights Act of 2020*.

[64] 2021. *An Act Concerning Additional Protection of Data Relating to Personal Privacy*. Retrieved September 28, 2022 from https://leg.colorado.gov/bills/sb21-190

[65] 2022. *An Act Concerning Personal Data Privacy and Online Monitoring*. Retrieved September 28, 2022 from https://www.cga.ct.gov

[66] 2022. *Utah Consumer Privacy Act*. Retrieved September 28, 2022 from https://le.utah.gov/~2022/bills/static/SB0227.html

[67] 2022. *Virginia Consumer Data Protection Act*. Retrieved September 28, 2022 from https://law.lis.virginia.gov/vacode/title59.1/chapter53/