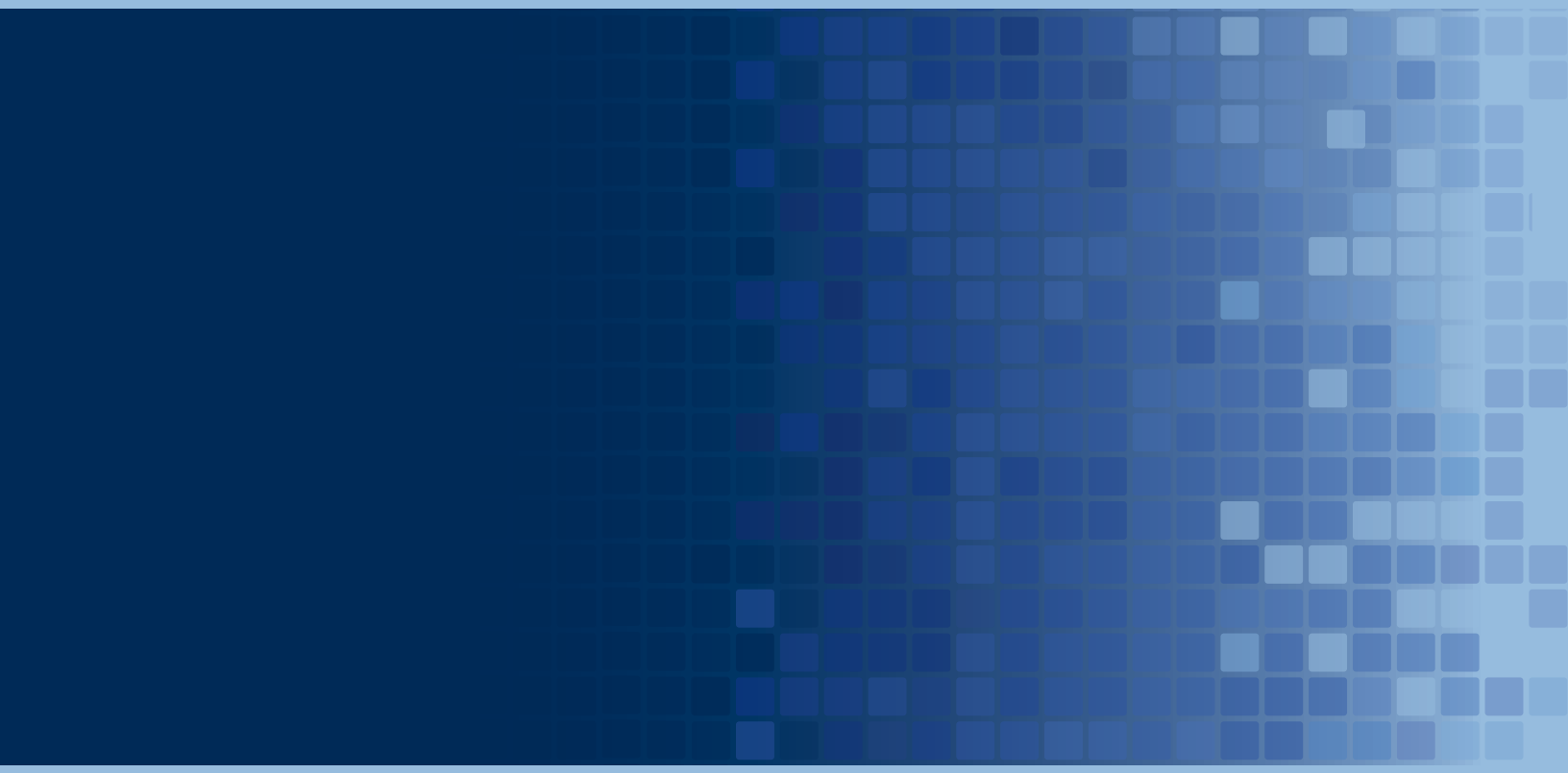
Governance Studies
at BROOKINGS

BRIDGING THE GAPS

A path forward to federal privacy legislation

By Cameron F. Kerry, John B. Morris, Jr.,
Caitlin T. Chin, and Nicol E. Turner Lee

June 2020



Preface

Despite a promising start in the 116th Congress, comprehensive information privacy legislation appears stalled on Capitol Hill. Although key Senate and House leaders on both sides of the aisle have put forward bills that reflect considerable consensus, there has been little movement on a few pivotal and more polarized issues.

To help inform the privacy debate and chart a path forward, this report presents a comprehensive review of key legislative proposals and offers detailed policy recommendations with the ultimate goal of filling in gaps in U.S. information privacy protections. Taken in its entirety, this report builds on principles and provisions in existing legislative proposals, while tackling some of the more contentious issues.

These recommendations include federal preemption of conflicting state laws on data collection, processing, and sharing, as well as a right for individuals to bring lawsuits for statutory violations. They integrate with our approach to other issues in privacy legislation, including algorithmic decision-making, civil rights, and limits on data processing. Our recommendations aim to prompt a clearer shift in regulatory paradigm by setting boundaries on how covered entities collect, process, and share personal information; establishing organizational accountability mechanisms; and graduating obligations according to the scale of the covered entity, covered data, and privacy risks involved.

Table of Contents

Introduction and Executive Summary

A. Background

In November 2019, Senator Maria Cantwell (D-WA) introduced the Consumer Online Privacy Rights Act (COPRA) and Senator Roger Wicker (R-MS) released the draft United States Consumer Data Privacy Act (USCDPA).[1]

As we (Kerry) wrote at the time, these two Senate Commerce proposals "frame[d] the issues for this discussion going into the next session of Congress" and introduced clarity to the broader privacy debate.[2] Shortly after, House Energy and Commerce Committee staffers circulated a "bipartisan staff discussion draft" for comment and, more recently, Senator Jerry Moran (R-KS) introduced the Consumer Data Privacy and Security Act (CDPSA).[3]

Our report seeks to unfreeze the privacy debate by exploring and offering a middle ground.

Although there is abiding interest in privacy legislation, member-level energy for bipartisan privacy negotiations has largely waned since the introduction of COPRA and USCDPA. Recently, response to the COVID-19 pandemic has necessarily consumed most of the available bandwidth in Congress. Yet the pandemic has raised issues surrounding access to mobility and proximity data, health information, and other forms of personal information that may—and in some cases may not—be useful for public health.[4] These are a reminder of the gaps in the U.S. system of privacy protection.

COPRA and USCDPA are promisingly similar in many aspects, with general stakeholder agreement on several significant issues. Even so, many stakeholders have staked out polar all-or-nothing positions on the two issues where Wicker and Cantwell are the furthest apart—federal preemption of state privacy laws, and a right for individuals to bring lawsuits for privacy violations. And so long as these protagonists remain in their own corners, the broader privacy debate will be frozen and federal legislation stalled.

Our report seeks to unfreeze the privacy debate by exploring and offering a middle ground. It proposes solutions on federal preemption and private lawsuits that depart from the maximalist approaches shaping the current debate. The report also articulates some

broad privacy protections that come with legal consequences but allow flexibility in compliance.

In our policy recommendations, we propose latitude for state laws by preempting them only where they interfere with federal provisions on data collection, processing, transfers, and security—and not altogether. Similarly, we suggest that individuals be allowed to file private lawsuits in court—but with substantive and procedural requirements to focus and filter these cases. Because the resolution of these pivotal sticking points—preemption and the private of action—cannot be achieved in isolation from the substantive requirements in a bill, our report analyzes the full scope of COPRA and USCDPA in the broader context of a comprehensive approach to protecting information privacy.

B. Overview of Recommendations

GRADUATED APPROACH TO RISK AND OBLIGATIONS

Woven throughout this report is an adaptive regulatory model that scales privacy and security obligations according to the covered entity, covered data, and privacy risks involved. As the scale of covered entities increases, the proposed obligations become more specific. Federal privacy legislation should not broadly exclude small businesses; rather, all covered entities should be subject to baseline obligations to limit data collection and processing, protect data security, and assess privacy risk "appropriate to the size and complexity of the covered entity and volume and nature and intended uses of the covered data processed." Both COPRA and USCDPA apply baseline, scaled data security standards for all covered entities, an approach we propose to adapt to other provisions.

Instead of prescribing specific limits or processes, we propose incorporating basic privacy protections into a duty of loyalty and duty of care that all covered entities must follow. The duty of loyalty would legally require covered entities to respect the privacy of individuals, including by implementing measures for data minimization, fairness, and transparency. The duty of care would legally prohibit covered entities from causing foreseeable injuries to individuals, including financial harms, privacy invasions "highly offensive to a reasonable person," and violations of anti-discrimination laws *(See Part II(A) of this report)*. The goal of this trade-off between flexibility and exposure is to focus attention on risk management and outcomes rather than delineate processes.

On the other hand, small and medium entities should be exempt from mechanisms that demand significant engineering or personnel, such as the rights of data access, correction, deletion, portability, and our proposed "right to recourse." Similarly, these organizations should be carved out of a requirement to appoint privacy and security officers. A scaled approach accepts that one size does not fit all when it comes to privacy; organizations are diverse and use data under a wide range of circumstances.

Another aspect of scaling is graduated effective dates of legislation. Unless otherwise provided, provisions should take effect upon enactment so that Federal Trade Commission (FTC) authorities immediately come into force. To allow covered entities enough time to come into compliance, however, we recommend that duties and obligations of covered entities apply six months after enactment, and that individual rights of access, collection, deletion, portability, and recourse enter into force after two

years. In turn, to leave time for the FTC to complete all required rulemakings, and effectively create a two-year period before full implementation (as with GDPR), federal and state enforcement should kick in six months after the relevant provisions take effect, and private lawsuits should not commence until implementation is complete.

Table 1: Baseline duties
Organizations require clear boundaries for how they can collect, process, and share personal information.

Provision	Covered Entity Obligations	Covered Entity Considerations	Covered Data Considerations	Privacy Risk Considerations	Intended Outcomes
Duty of loyalty	Establish reasonable policies and practices to minimize data use and provide transparency.	Obligations depend on the size and complexity of the covered entity.	Obligations depend on volume, nature, and intended uses of covered data.	Obligations depend on the potential impact on the privacy of individuals.	Process and transfer data in a manner that respects the privacy of individuals.
Data security	Establish, implement, and maintain reasonable data security practices to protect covered data.	Obligations depend on the size,complexity, and vulnerabilities of the covered entity, and the costs and technical feasibility of mitigating vulnerabilities.	Obligations depend on the volume, nature, and vulnerabilities of covered data.	Obligations depend on the potential risks to individuals from any unauthorized access, use, destruction, or disclosure of covered data.	Protect the confidentiality, integrity, and accessibility of covered data.
Risk assessments	Conduct privacy risk assessments that are reasonable and appropriate in scope and frequency.	Obligations depend on the size and complexity of the covered entity.	Obligations depend on the volume, uses, nature of the covered data.	Obligations depend on the potential risks to individuals from the collection, processing, and transfer of covered data by the covered entity.	Consider benefits, potential consequences, and measures to mitigate any consequences of data collection, processing, and transfers.

HEIGHTENED FOCUS ON OBLIGATIONS OF COVERED ENTITIES

A key objective of federal privacy legislation is to shift the burden of protecting personal information from individuals to the businesses that collect and use the information.[5] Both Wicker and Cantwell have said the current privacy system is "confusing" and "no longer enough,"[6] but their draft bills nevertheless frame the operative provisions first and foremost as "rights" for individuals. By contrast, we believe legislation should sharpen the focus on obligations of covered entities.

To reduce the burden on individuals, therefore, legislation should seek to minimize the number of times individuals are asked to review consent requests

and ensure that consent can be meaningful in situations where it matters most. Otherwise, legislation will end up perpetuating the existing failures of notice-and-consent.[7] Thus, while we accept requiring organizations to obtain affirmative express consent to process sensitive data, we suggest narrowing the definition of "sensitive data." To heighten the focus on how organizations handle personal information, our proposed duty of loyalty incorporates basic limits on data processing and transfers to purposes "reasonably foreseeable within the context of the relationship between the covered entity and an individual" *(See Part II(A) of this report)*. This concept of context, extrapolated from Section 105 of USCDPA, can also be applied in connection with when organizations should notify individuals of privacy policies.

We also see a need to differentiate more clearly between transparency provisions directed to individuals and those directed to regulators and privacy watchdogs. Privacy notifications to individuals—for affirmative express consent or other applicable purposes—should be to-the-point and offer clear and actionable choices, with the option to access other publicly-available but separate information about data collection and individual rights ("privacy statements"). The latter privacy statements also should be distinct from what we term "comprehensive disclosures," which primarily provide value to regulators and privacy watchdogs.

In addition to these obligations, we recommend that all covered entities have a general obligation to conduct "reasonable and appropriate" privacy risk assessments. Separately, large entities should be subject to a more specific requirement to conduct impact assessments before deploying algorithmic tools that can have significant effects on individuals, and to audit outcomes from these tools.

TAILORED PREEMPTION OF "INCONSISTENT" STATE LAWS

COPRA (Section 302) provides a roadmap for addressing preemption, but it is too narrow. It contains a savings provision for a variety of state statutory laws of general applicability, a separate one for state rights of action, and then a preemption provision aimed at "directly conflicting" state laws. However, the latter provision is largely negated by a further provision that a state law "shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under this Act."

> A key objective of federal privacy legislation is to shift the burden of protecting personal information from individuals to the businesses that collect and use the information.

With important changes, this general structure can provide a consistent national privacy standard while leaving significant room for state laws that fill gaps in federal law or address traditional state interests. For such changes, we recommend preempting "inconsistent" state laws that regulate the collection, processing, sharing, and security of covered data, and omitting the open door for more protective state laws. We also suggest increasing flexibility for both federal preemption and state laws by authorizing the FTC to preempt any state law that "directly conflicts" with the federal law and by providing for a limited eight-year sunset on preemption. A sunset provision would give Congress the opportunity to revisit any need for state laws to supplement a comprehensive federal privacy law, based on experience and issues that emerge following enactment.

TARGETED PRIVATE LITIGATION

Our private right of action recommendations are scaled based on injury to individual privacy interests and the proposed duties of loyalty and care. We generally recommend limiting recovery to "actual damages" and making a civil action under the federal law the exclusive remedy for the claimed privacy harms. Plaintiffs should be required to demonstrate a heightened standard, "knowing or reckless disregard," to sue for violations of substantive privacy provisions. However, any harms specifically identified under the duty of care, which have been commonly compensable under existing laws, should not be subject to this heightened standard. To avoid ratcheting up exposure for more technical statutory violations—that some characterize as "gotcha" cases—we suggest requiring plaintiffs to demonstrate "willful or repeated" offenses in order to sue for more administrative violations. Although recovery for most civil actions should be limited to "actual damages for the injuries," we propose that courts could award statutory damages of up to $1,000 per day if a plaintiff proves a "willful or repeated" violation. For class-action lawsuits, we suggest that limitations imported from the Private Securities Litigation Reform Act of 1995 could serve as a check to ensure that cases will benefit individuals in a class.[8]

If discrimination results from the collection and use of personal information, it becomes an information privacy issue.

Both to assist individuals and minimize unwarranted lawsuits, our recommendation also includes ways to avoid litigation. Before bringing a lawsuit, an individual plaintiff would need to exercise a "right to recourse," which is a proposed form of "notice and opportunity to cure" adapted from a variety of state statutes addressing consumer protection or unfair and deceptive acts and practices. This requirement would give people a simple way to address a range of privacy concerns, without needing to resort to litigation or convince an enforcement agency to act. At the same time, the requirement would give responsible entities an opportunity to address an issue before it turns into litigation. More than 5,000 companies have committed to a similar mechanism by signing up for the EU-U.S. Privacy Shield framework that enables transfers of personal data from the European Union.[9] If the suggested recourse mechanism does not resolve the issue, a legal complaint would have to include an affidavit attesting to the exercise of recourse and to facts that meet the pleading requirements of the different categories of violations.

ALGORITHMIC DISCRIMINATION

As the scale and complexity of machine learning and algorithmic decision-making grow, they generate increasing concerns about their potential effects on individuals. Above all, these concerns focus on whether algorithms can compound existing forms of societal discrimination—for example, from unrepresentative or incomplete training datasets or erroneous logic in data analysis or system design. Algorithmic discrimination is relevant to information privacy: if discrimination results from the collection and use of personal information, it becomes an information privacy issue.

Correspondingly, algorithms present challenges in interpretation under current anti-discrimination laws, which were written to address discrimination by human decision-makers. Both COPRA and USCDPA contain provisions on algorithms that recognize, in different ways, that such concerns may implicate federal anti-discrimination laws. We believe these differing provisions can be combined to make the FTC an effective adjunct to the federal agencies currently charged with federal anti-discrimination enforcement, with changes in language to adapt existing discrimination standards to the task of understanding how algorithmic decisions are made.

We also suggest separating COPRA's Section 108 on civil rights and algorithmic decision-making into two distinct sections. With this, we seek to broaden consideration of the potential effects of artificial intelligence beyond unlawful discrimination, and to increase accountability for these systems by requiring large data holders to conduct impact assessments and audits when deploying algorithmic decision-making systems that may have "significant effects" on individuals.

ORGANIZATIONAL ACCOUNTABILITY

It is important to have strong processes in place to ensure that covered entities take their privacy obligations seriously, and to engage the attention of top management on these obligations. We propose that all covered entities—even small and medium entities—conduct risk assessments that analyze "the benefits of its covered data collection, processing, and transfer practices; the potential adverse consequences of such practices to individuals and their privacy; and measures to mitigate any such adverse consequences." Consistent with the scaled approach we suggest, such risk assessments should vary in scope and depth depending on the nature of the covered entity, covered data, and the potential privacy risks. Large data holders, in turn, should be required to conduct more in-depth and extensive risk assessments and retain written copies of the assessments for at least five years.

In addition to risk assessments, most covered entities, except for small and medium entities, should designate at least one privacy officer and one data security officer. These corporate officials should develop written privacy and data security programs to guide the entity's compliance with the privacy legislation. Finally, the chief executive officers of large data holders, as well as privacy and data security officers, should annually certify to the FTC that the large data holder's annual disclosure of privacy practices is accurate and effective.

SAFETY VALVES

A federal privacy law cannot resolve all the issues of privacy protection—as we are seeing from the privacy, security, and technology issues arising out of the COVID-19 pandemic, the landscape is complex and rapidly evolving.[10] To take continuous change into account, Congress can provide for future reports to help evaluate the existing sectoral silos in federal privacy law. As in USCDPA (Section 403), we also suggest a mechanism for "approved certification programs" that would enable stakeholders to develop sector-specific guidance on how to comply with federal privacy legislation, subject to strong FTC oversight. Furthermore, our partial eight-year preemption sunset suggestion would force the political process to evaluate whether the federal law is working—and if Congress takes no action after eight years, stronger state laws could go into effect.

Table 2: Obligations of covered entities
We propose scaled obligations; no covered entity is exempted across-the-board.

Type of Obligation	Large Data Holders	Other Covered Entities	Small and Medium Entities
Duty of loyalty	✔	✔	✔
Duty of care	✔	✔	✔
Basic privacy statements	✔	✔	✔
Opt-out of transfers	✔	✔	✔
Consent to processing of sensitive data	✔	✔	✔
Consent to processing involving minors	✔	✔	✔
Consent to material changes	✔	✔	✔
Scaled data security obligations	✔	✔	✔
Civil rights	✔	✔	✔
Scaled privacy risk assessments	✔	✔	✔
Comprehensive disclosures	✔	✔	✔
Right to control	✔	✔	✘
Right to recourse	✔	✔	✘
Privacy and data security officers	✔	✔	✘
Written documentation of privacy risk assessments	✔	✘	✘
Executive certification of comprehensive disclosures, internal controls, and reporting structures	✔	✘	✘
Algorithmic decision-making impact assessment	✔	✘	✘

C. A Path Forward

These recommendations reflect a somewhat different regulatory model from most proposals. The baseline duties that we see underlying many of the obligations of covered entities and our private right of action proposal descend directly from a common law standard of reasonable care that differs from the more a priori approach of the European Union's General Data Protection Regulation (GDPR) and calls for case-by-case application. We think this approach makes sense because baseline federal privacy legislation must cover a broad spectrum of activities, and there are almost infinite variations in data collection and use in the context of rapid technological change.

Both businesses and consumer advocates may be concerned with the flexibility this model would allow and the uncertainty that could result. Some businesses might be anxious about complying with standards that do not translate into predictable checklists. Some advocates may see flexibility as a loophole that unscrupulous companies could exploit. Yet, flexibility enables agility and innovation for industry, while for advocates, the enforceable duties of loyalty and care can counteract exploitation.

We submit that both sides of the policy debate have something to gain from the balance struck—and both have something to lose from continued inaction and stalemate. Businesses have come a long way in recognizing that strong privacy legislation is important to promoting trust in their brands and competitiveness in national and international markets—but the longer industry holds out for sweeping preemption without any individual remedies, the harder a consistent national standard becomes to achieve.

On the flip side, reliance by advocates on state-by-state legislation is destined to leave an incomplete and haphazard set of protections for Americans. It took over 15 years for all 50 states to adopt data protection laws as basic as breach notification.[11] A similar path forward, simply put, would provide less comprehensive and meaningful privacy protections over a longer timeframe than what may be achievable at the federal level in the near future—if industry, advocates, and political leaders are willing to make some hard choices. We hope our broad but carefully calibrated compromises can point toward steps key stakeholders can take to reach effective national protection of information privacy.

D. Methodology

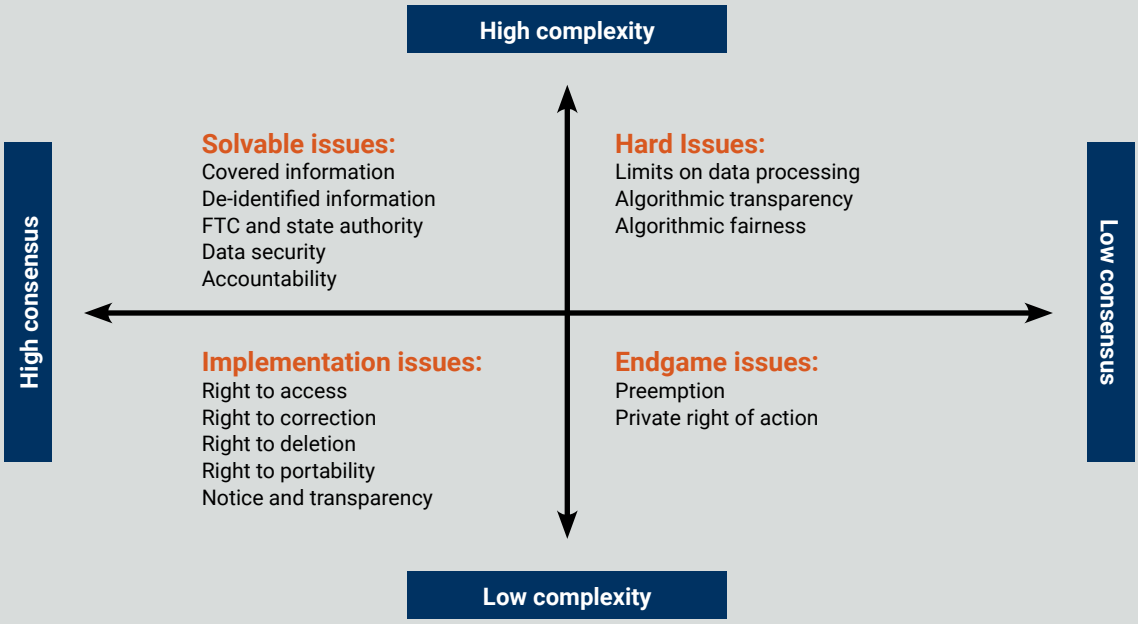
The Privacy Debate initiative at The Brookings Institution "brings together pre-eminent thought leaders on privacy, information security, and the digital economy to inform the growing national debate about individual privacy."[12] This report has been guided by our work on privacy, artificial intelligence, telecommunications, and emerging technologies, and we have expressed some of the ideas here in other publications at Brookings and elsewhere.

Alongside this writing and research, we have conducted numerous conversations with Capitol Hill staffers on both sides of the aisle and with a broad spectrum of stakeholders and experts across all sectors.[13] These include a series of focused, private roundtables with representatives of industry and civil society to explore issues of convergence and divergence in the privacy debate. While these participants have a diverse range of interests and positions that cut across various lines, we group them together as "industry" and "advocates" for the purposes of this report.

We submit that both sides of the policy debate have something to gain from the balance struck—and both have something to lose from continued inaction and stalemate.

Through these discussions and our analysis of privacy bills, frameworks, and policy positions, we characterized the privacy debate with a matrix that categorizes major issues based on the degree of consensus or disagreement along one axis, and the complexity—both substantive and political—of resolving areas of disagreement along another axis. In one quadrant, we have the "endgame issues," which are substantively well understood but see deep divides. This is where preemption and private right of action fit. Next are the "hard issues," which are both substantively complex and highly contested due to their impact on both privacy and business practices. The "solvable issues" are those in which

Figure 1: Key Issues in Federal Privacy Legislation



we see general, high-level agreement, but where the details are especially important. Finally, we call issues that are largely non-controversial and less complex the "implementation issues," as adopting them is primarily a matter of working out technical details. This matrix guides our continued focus on the key issues at stake.

Based on the matrix described above, this report begins with the endgame issues of preemption and private right of action. It then addresses the hard issues of limits on collection, use, and sharing of personal information, as well as discriminatory uses of personal information and fairness in algorithmic decision-making. The final two sections, the solvable issues and implementation issues, address the scope of information and entities that federal privacy legislation should apply to, federal and state enforcement powers, and the operation of individual rights.

At the outset of our process, we tabled discussion of preemption and private litigation for later—these two issues were futile until there was significant agreement on the contours of substantive privacy protections (which is why we dubbed them "endgame" issues). After the release of USCDPA and COPRA, however, we found a surprising degree of comfort across the spectrum of stakeholders—not only with their provisions on more technical issues such as the right to access personal information,

but also on more complex issues like limits on how covered entities can collect, process, and transfer data and how legislation is enforced. In that light, we concluded the time was ripe to explore what sort of limited private litigation rights industry might live with—and what limits on such rights advocates might accept.

Our recommendations emerge organically from these discussions and our years of experience thinking about—and drafting—privacy legislation. To prepare this report, we drew on a range of legislative proposals to weigh, line-by-line, how to bridge the differences in COPRA and USCDPA and distill our thinking into concrete text.

Bridging the Gaps: Key Recommendations

- **Preemption:** Consistent national privacy standards would benefit both individuals and industry. Today's digital society is not confined within state borders, and a person's privacy should not depend on which state they are in. We therefore recommend preempting "inconsistent" state laws that regulate the collection, processing, sharing, and security of covered data, while leaving space for the body of state laws developed over more than 100 years. We also recommend enacting a partial eight-year sunset provision for preemption, which would give Congress the opportunity to revisit the efficacy of federal privacy legislation and evaluate any necessity for supplementary state laws.

- **Private Right of Action:** Individuals should be able to seek redress for widely recognized injuries, but we generally recommend limiting recovery to "actual damages," requiring a heightened "knowing or reckless" liability standard for most statutory provisions, and requiring a "willful and repeated" standard to bring a private lawsuit for more procedural provisions. Procedural filters should include notice and an opportunity to cure, heightened pleading, and class-action limits adapted from securities litigation.

- **Limits on Processing:** Boundaries on collection, use, and sharing of personal information are essential elements of privacy protection. Data minimization provisions in existing bills can be combined into "duty of loyalty" and "duty of care" provisions that more broadly require covered entities to respect privacy, communicate policies fairly and transparently, and exercise reasonable care to avoid specified and well-recognized harms, including violation of anti-discrimination laws.

- **Consent, Notification, and Transparency:** We agree organizations should have to get affirmative express consent to collect or transfer sensitive data but recommend minimizing consent requests by narrowing the definition of "sensitive data" and focusing on what individuals can reasonably expect in "context." Covered entities should provide transparency in three layers instead of one-size-fits-all: a) timely, context-specific notifications for individuals, b) basic privacy statements targeted to individuals, and c) comprehensive privacy disclosures aimed at regulators and other close observers.

- **Graduated Obligations and Accountability:** Small businesses should not be exempt from comprehensive federal privacy legislation, as some have caused serious privacy and security failures. But small and medium entities (including smaller nonprofits) should be exempt from specific obligations that come with significant compliance costs. Basic underlying obligations—like the duty of loyalty, data security, and privacy risk assessments—should apply to all organizations but be tailored to the scale of the covered entity and the volume and nature of data involved. Additional obligations should apply to "large data holders."

- **Civil Rights:** Existing federal anti-discrimination laws, designed for human decision-making, need reinforcement to address automated decisions. Comprehensive privacy legislation should address algorithmic discrimination because covered data can be used in ways that disadvantage individuals. However, privacy legislation should not alter existing federal or state anti-discrimination laws, and the agencies currently tasked with anti-discrimination enforcement (e.g., the EEOC) should maintain their primary roles. The FTC should refer discrimination cases to the relevant federal agency, and privacy legislation should also prohibit the use of covered data in ways that violate existing anti-discrimination laws.

- **Individual Rights:** We recommend combining the individual rights to request access, correction, deletion, and portability of personal information into an overarching "Right to Control" section and adding a separate "Right to Recourse" that would have to be exercised prior to bring litigation.

Part I — The Endgame Issues

The path to privacy legislation goes through preemption and private right of action, which is why we begin with the "endgame issues." Stakeholders are generally polarized on these issues, yet they must be addressed if privacy legislation is to become law. In this part of the report, we seek to navigate the concerns that entangle these stubborn issues. Our recommendations will not satisfy maximalists on either side of the debate, but we hope that they may address legitimate interests of divergent stakeholders in ways that allow them to bridge these gulfs.

KEY RECOMMENDATIONS:

- Today's digital society and economy are not confined within state borders, and both organizations and individuals would benefit from a single set of national privacy rules. We recommend preempting "inconsistent" state laws which regulate the collection, processing, sharing, and security of covered data, including inconsistent state laws that "afford a greater level of protection" than a federal law.

- To encourage Congress to revisit privacy legislation, we recommend adopting an eight-year partial sunset provision for preemption.

- To allow individual redress for widely-recognized injuries and supplement public enforcement of privacy legislation, we propose a private right of action generally limiting recovery to "actual damages," but with statutory damages of up to $1,000 per day available for "willful or repeated" violations. Other than for violations of the duty of care—which should not be subject to a heightened standard—individuals should be required to demonstrate a "knowing or reckless" violation to sue for most statutory provisions and "willful or repeated" violations to sue for more technical or administrative provisions.

- To prevent excessive litigation and give both individuals and organizations a simple way to address privacy disputes, potential plaintiffs should be required to exercise a "right to recourse" before bringing private lawsuits for information privacy violations. Other procedural recommendations include, for example, requiring complaints to allege violations of the statute with "reasonable particularity" and incorporating additional pleading requirements for class actions.

The path to privacy legislation goes through preemption and private right of action, which is why we begin with the "endgame issues."

A. Preemption

Preemption, like the private right of action discussed in Part I(B) of this report, can be an article of faith on both sides. Justice Brandeis celebrated the role of state laws by famously stating, almost 90 years ago, that a state may "serve as a laboratory … and try novel social and economic experiments without risk to the rest of the country."[14] In the modern privacy realm, many advocates celebrate Brandeis's description and resist any prospect of closing off state legislative action. Especially in the face of industry resistance and congressional inaction, state legislatures have taken the lead on privacy legislation, and advocates hope for a steady march forward from California and Illinois to other states.[15]

In turn, the single most important reason for industry to accept and support federal privacy legislation is an understandable desire for a single national set of rules to follow. Especially as the national and global internet operates across state borders, industry leaders want to avoid differing and potentially conflicting state laws that would set privacy rules based on a user's residence or current location.[16]

The preemption provision in USCDPA (Section 404) is brief and broad. With the sole exception of data breach laws, the proposed text would enact "field preemption" to supersede all state laws and regulations "related to the data privacy or security and associated activities of covered entities." Such a provision would sweep away a body of state privacy laws developed over decades, including some that address issues that are wholly offline and within a single state. For example, states have laws concerning the privacy and security of educational, library, and insurance records, among many other topics that affect a range of predominantly local interests.

COPRA (Section 302) preempts "directly conflicting" state laws, while preserving a variety of state statutes of general applicability and state rights of action, providing a useful roadmap to address preemption. However, the preemptive impact is largely negated by an additional provision that a state law "shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under this Act."

Taken together, COPRA's approach would undermine the goal of a national standard for privacy practices, compliance systems, and consumer expectations. The risk of a patchwork of differing state laws—which may conflict with each other, even if they do not conflict with a federal law—undermines the goal of strong privacy protections for all Americans. As a matter of political reality, a profusion of state privacy laws may complicate rather than motivate the prospect of congressional enactment.

In evaluating the competing interests of advocates and industry—to protect states' ability to innovate on privacy protections and avoid a patchwork of regulation, respectively—we propose a path that preempts state laws that compete with a national standard, preserves other state privacy laws and rights, and prompts Congress to revisit this question after experience with the new federal law.

Ultimately, we are persuaded that the internet and the applications and services that run on it are more

like railroad and automobile standards, which are largely subject to federal regulation, rather than the insurance industry, which is largely regulated by states. We also believe that a preemptive national law with effective privacy protections is more beneficial for people everywhere in the United States compared to no national law or a weak national law without preemption.

We think that the current privacy debate presents a genuine opportunity to achieve meaningful privacy protections on a national basis. We also believe that significant preemption is the price to pay in exchange for establishing strong privacy protections for all Americans. Because we recommend preserving a robust role for states in the enforcement of federal privacy legislation (as COPRA and USCDPA provide), we do not believe that a well-focused preemption provision would unduly impinge on states' ability to protect their residents.

A TIERED APPROACH TO PREEMPTION

As noted above, we believe that the general structure of COPRA's preemption language can be revised to provide a strong national standard for privacy while leaving significant room for state laws that fill gaps or address traditional state interests. We recommend several changes and additions to the language in COPRA:

State law preservation

To COPRA's good list of state laws to be preserved, we suggest adding state constitutional law and state laws relating to social security numbers, motor licenses, and public records. We recommend removing the preservation of state laws giving private rights of action. Finally, we would suggest a number of language tweaks and additions.

Preemption of "inconsistent" state laws

Our most significant modification to COPRA's preemption provision is to preempt "inconsistent" laws rather than only those that are "directly conflicting" and to omit the exception permitting state laws with a greater level of privacy protection than the federal law. Specifically, we recommend the preemption of state laws "regulating the collection, processing, sharing, and security of covered data to the extent such law is inconsistent" with the federal law or regulation.

This suggested approach aimed at "inconsistent" state laws is modeled on Section 536 of the Cable

Table 3: State Law Preservation
We recommend preserving the following state laws, regulations, and rules:

- Consumer protection laws of general applicability
- Laws prohibiting unfair and deceptive practices
- Civil rights laws
- Laws that govern employee, student, or library privacy
- Data breach notification laws
- Contract, property, or tort law
- Criminal laws governing fraud, theft, or other similar behavior
- Laws addressing social security numbers, motor or vehicle license information, or other public records
- Public safety laws
- Sector-specific laws unrelated to privacy or security
- State constitutional law

Communications Policy Act of 1984.[17] Cable television, like privacy, is a field in which federal law is overlaid on a body of existing state regulation. Although such issue preemption sets indefinite boundaries that may be defined on a case-by-case basis, federal law has dominated the shape of cable television regulation and, in our experience, most disputes about preemption have been resolved by accommodation. A somewhat narrower "directly conflicting" standard, we believe, would likely lead to a greater patchwork or overlap in privacy regulation[18] and result in more uncertainty and disputes parsing whether a state statute "conflicts" with a national law, and does so "directly."

Our approach to preemption strikes a constructive balance among the competing goals of establishing strong national privacy standards, preserving longstanding state laws, and ensuring continued focus on privacy.

Federal Trade Commission regulatory authority

To provide a faster and easier method than litigation for resolving uncertainty about whether a state law conflicts with a federal law, we recommend giving the FTC authority to resolve questions about preemption either in response to a petition or on its own accord. To avoid excessive preemption, we suggest that the FTC's ability to preempt a state law be limited to the extent "necessary to prevent such conflict," thereby requiring the Commission to leave in place a state statute as a whole when a small preemptive action can reconcile any inconsistency.

In addition, we suggest the FTC be able to use preemption power to address laws of two or more states when they "conflict with each other in a manner that harms the goals or operation of [the federal privacy law] and that creates a burden on interstate Commerce." With situations in mind that may arise under the partial sunset of preemption detailed next, the goal of this suggested language is to minimize situations where two or more states create conflicting obligations for covered entities that operate across state lines.

Partial sunset of preemption

We propose a sunset of one aspect of our recommended approach to preemption: after eight years, states would be permitted to enact privacy rules that provide *greater* protection than the federal law, leaving the federal law as a floor for privacy protection. Specifically, we suggest that a state law be permitted when it:

(i) is enacted eight years after the enactment of this Act;

(ii) states explicitly that the provision is intended to supplement this Act; and

(iii) gives greater protection to individuals than is provided under this Act.

The concept, text, and duration of this suggested preemption sunset is drawn directly from the 1996 amendments to the Fair Credit Reporting Act (FCRA).[19]

We believe that a partial sunset would serve two valuable purposes. First, it would ensure that there will be demand for Congress to revisit the success (or lack thereof) of the federal privacy regime, from the perspective of both enhancing privacy protections and fixing procedural or other problems that may arise with the law. In all likelihood, industry

stakeholders would lobby for elimination of the sunset (as occurred with the 1996 FCRA sunset),[20] while advocates would lobby to improve the federal law and protect the sunset. The resulting conversation before Congress would be valuable.

Second, the sunset provision provides a safety valve to address future privacy concerns in case Congress does not act. In this scenario, states could seek to address privacy problems that may have evolved over the eight years after enactment of a federal law, while the FTC would retain the ability to preempt state law provisions that undermine the federal privacy regime.

Taken together, we believe our approach to preemption strikes a constructive balance among the competing goals of establishing strong national privacy standards, preserving longstanding state laws, and ensuring continued focus on privacy. We believe that this balance, coupled with our private right of action recommendation set out below, can provide a path forward for stakeholders to find solutions toward successful comprehensive federal privacy legislation.

B. Private Right of Action

It is challenging to plot out a middle ground on whether individuals should be able to bring lawsuits for privacy violations. No issue in the privacy debate is as polarized. Private lawsuits—especially consumer class actions—are anathema even to privacy-friendly companies, while for many consumer, privacy, and civil rights groups, they amount to foundational goals.[21] In turn, these key party constituencies influence the positions of members of Congress.

COPRA and USCDPA reflect these polar positions. USCDPA contains no provision for a private right of action. COPRA does have one (Section 301(c)), and it allows for all forms of relief—including punitive damages, litigation fees, and statutory damages of $100 to $1,000 per day or the amount of actual damages—with no procedural or substantive limits to narrow claims. Senators Jerry Moran (R-KS) and Richard Blumenthal (D-CT) tried to negotiate a more limited provision but, as Moran's release of his own bill reflects, their effort ran into a wall.[22]

> Federal privacy legislation is unlikely to pass without some resolution of this issue (i.e., without a private right of action in some form).

These impasses make clear that federal privacy legislation is unlikely to pass without some resolution of this issue (i.e., without a private right of action in some form). Our discussions with stakeholders therefore focused on identifying key interests on each side of this divide and exploring what each may be able to live with. Based on this input and our related analysis of possible provisions, we recommend allowing individuals to pursue remedies for violations of baseline privacy legislation that directly and substantially affect them, but also suggest adding substantive and procedural filters to avoid unnecessary litigation.

In our discussions, advocates voiced two key reasons for allowing private lawsuits. One, not surprisingly, is to allow individuals to seek redress for injuries stemming from violations of legally-protected

privacy interests. The second is to supplement public enforcement of the statute by adding individuals as force multipliers to the FTC and state attorneys general. In turn, many industry representatives are not opposed to all litigation but are generally concerned about what they regard as nuisance lawsuits. In their view, there is also a potential for class actions and damage multipliers (like statutory damages, punitive damages, and multiple damages) to ratchet up the nuisance value of suits regardless of their merits. Each of these positions has some force.

There are some kinds of privacy injuries few would dispute should be compensable. For example, non-consensual pornography or the use of stalking apps or spyware against a former spouse or sexual partner.

There are some kinds of privacy injuries few would dispute should be compensable. For example, non-consensual pornography or the use of stalking apps or spyware against a former spouse or sexual partner. Similarly, there is little dispute that financial loss, such as the consequences of identity theft, should be capable of recovery—although the exact nature and extent of injury has been much debated.[23] These are the kinds of injuries that have had a history in common law and statutory law since Samuel Warren and Louis Brandeis wrote their foundational law review article, "The Right to Privacy," in 1890.[24]

Today, the privacy landscape in the United States contains many laws that allow individual lawsuits. The progenitor of federal privacy laws, the Fair Credit Reporting Act, allows individuals to sue reporting agencies and recover at least $100 or actual damages, punitive damages in cases of "willful or intentional" violations, and reasonable attorney's fees in all cases.[25] Its progeny—the Privacy Act, the Right to Financial Privacy Act, the Cable Communications Policy Act, the Electronic Communications Privacy Act, the Video Privacy Protection Act, and the Telephone Consumer Protection Act—all allow for individual lawsuits in various ways.[26] There is also a history of state statutes with remedies for express rights to privacy as well as common law torts for invasions of privacy interests. Furthermore, all fifty states have passed unfair and deceptive acts and practices (UDAP) laws, many of which provide for individual lawsuits.

When William Prosser organized privacy torts and the Warren and Brandeis "right to privacy" into four main categories more than 50 years ago, he noted "[t]he difficulty of measuring damages."[27] This difficulty persists today and is one reason that many of the federal laws previously enumerated include statutory damages in specific sums or ranges. These serve to vindicate privacy interests by ensuring a recovery for a prevailing plaintiff regardless of the actual damages.

The Telephone Consumer Protection Act (TCPA) has been particularly controversial in this regard. Although enacted to address pestilent robocalls, it turns on the use of auto-dialers more broadly and has thus hindered legitimate companies in contacting their own customers, created confusion over whether automated replies constitute autodialing, and led to claims based on processing do-not-call requests too slowly.[28] The TCPA allows a private right of action for up to $500 per violation, and some assert that this provision enables "gotcha" claims. In 2019, this statute produced the highest trial damages award under a privacy law—$925 million—in a class action against the multilevel marketer ViSalus, Inc.[29]

Everyone hates robocalls, but even privacy advocates may question whether they amount to one of the worst privacy offenses. The *Wakefield v. ViSalus, Inc*. verdict demonstrates how statutory damages, multiplied by a large number of class action members, can add up. Exposure like this gets the attention of C-suites and boardrooms because it can amount to enough to require reporting in litigation risk disclosures for securities filings and balance sheets. The effects of these multipliers were a key concern of companies we spoke with. Privacy class action lawyer Jay Edelson, whose firm litigated the *ViSalus* case, observes that privacy class actions tend to settle cases because of the amount of money involved and wide ranges in value. Even Edelson concedes that some statutory damages can be disproportionate, saying that the California Consumer Privacy Act's (CCPA) $500-per-violation penalty for data breaches is excessive in many cases.[30]

When it comes to private or public enforcement, we think governments are more able to provide policy coherence to enforcement—one reason we suggest below that the FTC be able to take over state lawsuits. Individual plaintiffs have no obligation to act in the public interest. And while Federal Trade Commission and state enforcement officials are subject to personal political interests, they do have such an obligation. It is a good idea to keep the civilian posse under the supervision of the marshal.

Nevertheless, the task of enforcing a federal privacy statute will be enormous—much greater than any existing sectoral regime. The arena comprises much of the information use and economic activity in the United States, affecting almost every person. Enforcement will require a significant increase in the composition of the FTC and, as we discuss in a later section, we recommend adding at least 500 personnel dedicated to privacy enforcement *(See Part III(D) of this report)*. Even with 500 additional employees, the FTC would be lean to compare to privacy enforcers in the Europe—the UK's Information Commissioner's Office alone has over 500 employees for a country with one-fifth the population of the United States.[31] Private litigation is imperfect, but it can serve as an incremental enforcement and policymaking tool. The common law tort system based on reasonable care has helped to improve the health and safety of workplaces, buildings, vehicles, drugs, and consumer products. The iterative process of case-by-case adjudication is part of our conception of a flexible and risk-based approach to protecting privacy.

The iterative process of case-by-case adjudication is part of our conception of a flexible and risk-based approach to protecting privacy.

A FOCUSED RIGHT OF ACTION

There are numerous ways to narrow the range of individual lawsuits to enforce a privacy law. The choice is not bound to either an unlimited private right of action or none at all. Options include (a) heightening liability standards, (b) limiting what provisions are enforceable through private lawsuits, (c) providing for notice and an opportunity to cure prior to bringing suit, (d) raising standards for pleading cases, (e) placing limits on damages, (f) shifting costs and fees, and (g) placing limits on class actions. We considered all of these and recommend adding elements of them all to the private right of action in COPRA.

Substantive rights

We incorporate a tiered approach to private enforcement by proposing different standards for different

provisions, which a plaintiff would need to plead in enough detail to meet the standard of "particularity."[32] We recommend three different tiers of liability, each requiring a well-established state of mind standard for differing categories of violations of the privacy statute.

The injuries covered by this duty of care are the kind widely recognized as compensable under the common law right of privacy, consumer protection statutes, and anti-discrimination laws. Thus, the duty would target specifically the kinds of injuries we suggest a private right of action reasonably should protect.

As described below, we recommend reframing the loyalty provisions that appear in Sections 101 of both COPRA and USCDPA—in different forms—into two broader duties of loyalty and care. Our proposed duty of loyalty would require covered entities to implement reasonable policies and practices to protect individual privacy "appropriate to the size and complexity of the covered entity and volume, nature, and intended use of the covered data processed," limit data processing to "necessary [and] proportionate" purposes, consistent with COPRA and USCDPA, and communicate data practices "in a fair and transparent manner." The duty of care would modify the "harmful data practices" specified in Section 101(b)(2) of COPRA by including "discrimination in violation of Federal anti-discrimination laws or anti-discrimination laws of any State or political subdivision thereof applicable to the covered entity," and prohibiting covered entities from processing covered data in a way that "reasonably foreseeably causes" the enumerated harms *(See Part II(A) of this report)*.

The injuries covered by this duty of care are the kind widely recognized as compensable under the common law right of privacy, consumer protection statutes, and anti-discrimination laws. Thus, the duty would target specifically the kinds of injuries we suggest a private right of action reasonably should protect. For violations of the duty of care, therefore, we do not propose any heightened state of mind standard. In other words, covered entities could still be held liable even if unaware of any violations of the duty of care, but would not be subject to a strict liability provision (as they might under COPRA's Section 101(a)(2) harmful data practices provision), because the element of reasonable foreseeability imports a negligence standard.

We then recommend treating the duty of loyalty and other substantive obligations—including consent, data security, and civil rights—under a standard of "knowing or reckless disregard for the privacy or security of individuals." Here, the goal is not to allow a lawsuit for each and every data security breach or failure to obtain affirmative express consent before collecting sensitive data, but to ensure that bad actors are not immunized.

To bring private lawsuits related to provisions outside of these provisions, we recommend requiring plaintiffs to demonstrate "willful or repeated" violations of the statute. This would apply to provisions affecting individual rights of access, correction, deletion, data portability, and other recourse; appointment of privacy and security officers; conduct of risk assessments; and comprehensive privacy disclosures. These are administrative provisions

that are important to accountability and effective privacy practices but might not necessarily have a direct impact on an individual's privacy protection. The "willful and repeated" standard would prevent "gotcha" suits for violations with no real impact on individuals, but help prevent patterns or practices of violating these accountability requirements or other flagrant disregard.

Damages

Apart from cases of "willful or repeated" violations of any provision, we recommend covered entities be insulated from statutory damages. Thus, for statutory violations that are not "willful or repeated," we would generally limit recovery to actual damages for the injuries established, plus attorney's fees, litigation costs, and any equitable relief a court awards in its discretion. One-time events may affect many people, such as when an organization changes its privacy policies, so it would be helpful to clarify that a violation is not considered repeated "solely by virtue of the fact that it affects a large number of individuals within a short period of time." This would exclude statutory damages for one-time events while leaving a door open to obtain statutory damages of up to $1,000 per day for violations that continue over some period of time.

As discussed above, questions about the nature and extent of damages have long been an issue in privacy litigation. In the online era, courts have addressed the constitutional issue whether plaintiffs meet standing requirements under Article III of the Constitution—which will also operate as a limiting factor to a federal right of action. For example, in *Spokeo, Inc. v. Robins* (2016), Robins brought a class action lawsuit under the Fair Credit Reporting Act of 1970—the first federal privacy statute—alleging that a "people search engine" displayed incorrect personal information about him and seeking damages.[33] The Supreme Court sent the case back to the lower courts to determine whether allegations of intangible harm were both "particularized" and "concrete" enough to present a case or controversy eligible for Article III purposes.

The *Spokeo* Court specifically recognized that "Congress is well positioned to identify intangible harms that meet minimum Article III requirements …." This invites Congress to articulate privacy harms.

In discussing these requirements, the Court noted that "concrete" injury must be "real, and not abstract," but also that the violation of "intangible" rights like free speech and free exercise of religion can count. Although the Court ruled that not every inaccuracy or procedural violation under FCRA amounts to concrete harm, it acknowledged that when considering "whether an intangible harm constitutes an injury in fact, both history and the judgment of Congress are instructive." The *Spokeo* Court specifically recognized that "Congress is well positioned to identify intangible harms that meet minimum Article III requirements …." This invites Congress to articulate privacy harms.

Doing so can help with standing hurdles but may not solve the challenges of establishing damages. In free speech and free exercise litigation, success often comes in the form of injunctive relief. Here, the availability of attorney's fees and costs can ease the burdens and disincentives in bringing constitutional

litigation and create exposure for defendants. Allowing courts to award reasonable litigation costs and attorney's fees for private lawsuits would serve the same purpose for privacy cases.

Procedural limits

We recommend several procedural rules to deter unmeritorious cases.

Based on the Massachusetts UDAP statute and (more loosely) on CCPA, we recommend a form of notice and opportunity to cure.[34] We conceive of it as tied to our proposed right to recourse, which we discuss in Part IV(B) of this report, but it could be adopted as an independent provision. The Massachusetts statute requires that a plaintiff first give the relevant business a 30-day notice of the claim and attest to the notice and failure to act before bringing a lawsuit for unfair or deceptive acts or practices.[35] Requiring individuals to pursue the right to recourse would give them a simple way to resolve claims, while also allowing covered entities a chance to head off litigation. We note that there should be an exception for situations, such as stalking, that present a risk of physical injury or other irreparable harm if an individual has to wait 30 to 45 days for a response to the recourse request. Since we recommend exempting small and medium entities from the right to recourse requirement, a 30-day notification of claim with time to respond (as under the Massachusetts UDAP statute) should be sufficient for an individual to sue smaller entities.

We received feedback that plaintiffs should be permitted to recover damages only after first obtaining an injunction that has been violated. The trouble with such a prerequisite is that it could block some of the cases that most deserve compensation. Take, for example, someone who has suffered identity theft leading to tangible financial loss—an injunction would have limited effect after the fact, yet compensation would not be available if the injunction is not violated.

While we do not think a privacy law should be encumbered with so dramatic a change in the American allocation of litigation costs as to shift costs and attorney fees to the losing party, we do incorporate a modest fee-shifting provision that is consistent with well-accepted American law. It is modeled on offers of judgments in Rule 68 of the Federal Rules of Civil Procedure, which permits a civil defendant to make an offer that, if accepted, can be converted into a judgment against the defendant, but if rejected, can shift liability for litigation costs if the plaintiff fails to recover more than the offer.[36] Based on this model, we propose that a covered entity responding to a request for recourse be able to offer money, and that this offer function like a Rule 68 offer if a plaintiff eventually recovers less than the amount of the offer. Like Rule 68, this would serve to promote the settlement of claims.

In early November, Representatives Anna G. Eshoo (D-CA) and Zoe Lofgren (D-CA) introduced the Online Privacy Act, which would limit class actions to cases brought on behalf of individuals by nonprofit organizations (as does CCPA), thereby cutting out the class action bar.[37] As with fee-shifting, we do not see why privacy cases should be treated very differently from other litigation, but we do find limitations in existing law that could be included in a private right of action provision. The Private Securities Litigation Reform Act of 1995 (PSLRA) establishes additional pleading requirements for securities litigation that serve to hold discovery at bay until a class is approved.[38]

It also spells out procedures for selecting a lead plaintiff among class representatives and outlines the class benefits and expected fees in class settlements. These procedures can be adapted to privacy litigation, leaving out some provisions that are sui generis to securities cases. Since the PSLRA refers to Rule 23 of the Federal Rule of Civil Procedure, which governs class actions, we think such a provision in privacy legislation would need to give the federal courts exclusive jurisdiction over class actions; overlaying it onto state litigation could prove excessively complicated.

In a similar vein, we recommend that the federal right of action be the exclusive remedy for the actions complained of in all private lawsuits. This would preclude appending more expansive state claims to a federal case, forcing an election of remedies. It would also prevent bypass of the damage limits under federal law on the basis of state claims.

COPRA does not include a statute of limitations with its private right of action provision. We recommend including one and would opt for the limitations period governing bank records in the Right to Financial Privacy Act: three years from the date of the violation or from the date of discovery, whichever comes later.[39]

Barring a radical change in the make-up of Congress, the issue of a private right of action in federal privacy legislation is unlikely to be resolved with an either/or outcome.

Barring a radical change in the make-up of Congress, the issue of a private right of action in federal privacy legislation is unlikely to be resolved with an either/or outcome. As a result, enacting comprehensive baseline legislation will require choices. Given the options for tailoring a private right of action, such choices would likely bear some resemblance to what we suggest here.

Part II — The Hard Issues

KEY RECOMMENDATIONS:

- The FTC should have broad jurisdiction to enforce privacy rules as consistently as possible, including over common carriers, nonprofits, and small businesses. Small and medium entities (including small nonprofits) should be exempt from some process obligations.

- All covered entities should be subject to a baseline "duty of loyalty" and "duty of care" provision that requires covered entities to respect the privacy of individuals and limit data use to purposes "reasonably foreseeable" within a given context, communicate policies fairly and transparently, and follow existing anti-discrimination laws, among other provisions.

- Although consent places a well-documented burden on individuals, affirmative express consent for collection or transfers of "sensitive" data is an enduring element of privacy legislation. To minimize "consent fatigue," the definition of "sensitive data" should be more narrow and other notification requirements more context-dependent.

- Privacy legislation should address algorithmic discrimination because covered data can be used in ways that disadvantage individuals and because existing federal anti-discrimination laws, designed for human decision-making, need reinforcement to address automated decisions. The algorithmic discrimination provision should combine the USCDPA provision on FTC referrals to federal anti-discrimination agencies with the COPRA prohibition on using covered data in ways that discriminate.

- An anti-discrimination provision in a privacy bill should reference existing and future federal anti-discrimination laws, rather than specify protected categories, and should include language tailored to algorithmic decision-making. This should include a provision on disparate impact, because the covered entity that uses algorithmic decision-making is in the best position to assess an algorithm's impact and explain its decisions.

A. Limits on Processing of Covered Information

Privacy legislation has gained momentum in recent years from wide recognition that the current system allows unbounded collection, use, and sharing of personal data, and leaves companies largely able to set their own limits. The result is not only that companies are free to collect vast amounts of personal data, but they also can share it across a leaky information ecosystem comprised of many entities most people barely know exist, such as contractors, adtech providers, scoring agencies, and data brokers. From the standpoint of protecting individual privacy, setting boundaries for how covered entities can collect, use, and share personal information is the paramount issue for privacy legislation.

Setting such boundaries is challenging because of a number of tensions that are difficult to reconcile. As a society, we value the flow of information for its contributions to social intercourse, economic activity, and human knowledge. Indeed, as we maintain physical separation to combat the COVID-19 pandemic, we depend on such contributions more than ever. As individuals, we value the utility, connection, and convenience that come with the uses of personal information even as almost all of us have to make privacy compromises to obtain these benefits.

As a matter of policy and legislative drafting, it is difficult to specify boundaries because the contexts for data use—the kinds of data, the purposes and circumstances of the use, the nature of the entity receiving the data, and the entity's relationship with the individual—are infinitely variable. As a result, any definitive boundary or categorical list is apt to be over-inclusive or under-inclusive, and often both. The result is that a trade-off between certainty and flexibility is unavoidable in well-tuned privacy legislation. We prefer to err toward flexibility and fill gaps iteratively rather than prescriptively.

Finally, as a matter of politics, any limits on data collection, use, and sharing can have a direct impact on business models for advertising, data brokerage, and others that make up information-sharing ecosystems. This raises the stakes in setting boundaries on processing.

Considering these hurdles, USCDPA and COPRA are remarkably close together in their provisions on collection, use, and sharing of data. Both contain provisions on data minimization that are conceptually similar though expressed in different language; both require affirmative express consent for use or transfer of sensitive covered data and a way to opt out of the transfer of other covered data; and both would limit data transfers based on the "reasonable expectations" of individuals and address how service providers and third parties handle covered data.

From the standpoint of protecting individual privacy, setting boundaries for how covered entities can collect, use, and share personal information is the paramount issue for privacy legislation.

We believe it is possible to build on these approaches and bridge their differences in ways that would depart more clearly from our current inadequate system. The provisions in COPRA and USCDPA on collection, use, and sharing contain elements that can be combined to set more distinct, normative boundaries for the processing of personal

information and more emphatically shift the burden of protecting information privacy from individuals to the entities that process the information.

Despite promising elements, COPRA and USCDPA do not do enough to change the way data is collected and used today.

DUTIES OF LOYALTY AND CARE

Both COPRA and USCDPA begin with a series of data "rights" that include a "loyalty" provision (Section 101 in both) and go on to propose other limits on the collection and use of covered personal information.

Under the heading of a "duty of loyalty," COPRA's loyalty provision is significantly more expansive and incorporates several overlapping concepts. It prohibits covered entities from engaging in any "deceptive data practice," which is defined circularly as (1) any processing that amounts to an unfair or deceptive act or practice under the FTC Act, or (2) any processing or transfer that violates COPRA itself. Meanwhile, Section 301(a)(2) completes the circle by making any violation of COPRA also a violation of the FTC Act or any regulation promulgated under the FTC Act. In addition, Section 101 of COPRA prohibits any "harmful data practice," which is more concretely defined as a "financial, physical, or reputational injury to an individual;" as "physical or other offensive intrusion upon the solitude or seclusion of an individual or the individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person;" or as "other substantial injury to an individual."

This approach owes some debt to the Data Care Act that Senator Brian Schatz (D-HI) proposed late in 2018 to initiate a discussion about duties in privacy legislation.[40] Schatz is also a co-sponsor of COPRA and was a member of the bipartisan working group that worked for nine months on a privacy bill. The Data Care Act articulated broad provider duties of "care," "loyalty," and "confidentiality," and grouped some privacy obligations under these headings. In turn, that bill adapted the concept of "data fiduciaries" and created obligations to protect the interests of individuals in processing personal information. How to articulate such baseline duties toward individuals has been a matter of debate in subsequent negotiations among Senate Commerce Committee members.

Section 101 of USCDPA does not address loyalty in collection, processing, or transfer of data, but instead prohibits the denial of goods or services on the basis of the exercise of individual rights, as well as any waiver of these rights in a user agreement.

The keystone provisions on limits of collection and processing in COPRA and USCDPA—albeit separate from their respective loyalty provisions—are their sections on data minimization (COPRA Section 106; USCDPA Section 105). Both proposals limit the collection, processing, and transfer of covered data to what is "reasonably necessary, proportionate, and limited," and describe two broad categories of acceptable purposes. The first category includes data practices described in publicly-accessible privacy policies, which each bill additionally requires. The second category covers business purposes relating to products or services provided to an individual.

On the second category, the two drafts take different directions. COPRA lists permitted business purposes (Section 110) separate from its data minimization

section (Section 106). USCDPA addresses permitted business purposes within its data minimization section (Section 105) and allows for the collection and use "to provide or improve a product, service, or a communication about a product or service," including products that are both "specifically requested" or *"reasonably anticipated within the context of the covered entity's relationship with the individual."* For reasons discussed below, we believe the latter language is worth building on more boldly as a core concept for data processing limits.

Both COPRA (Section 110) and USCDPA (Section 108) spell out specific collection and processing purposes that are exempt from affirmative express consent and other requirements, such as fulfilling transactions, protecting security, and complying with legal obligations. Although the language differs, they are the same in substance, with the exception that USCDPA includes "internal research to improve, repair, or develop products, services, or technology" in this exemption. In this light, it is not clear why similar purposes are carved out in the data minimization language of that draft bill quoted above.

In light of the COVID-19 pandemic, it is notable that both bills call for the FTC to set oversight standards for "scientific, historical, or statistical research" that is "in the public interest," meets applicable legal and ethical standards, and undergoes oversight like that of an institutional review board. There may be value for enforcement and implementation purposes to having specific rules. But it is the Department of Health and Human Services that has mainly taken the lead on research standards—followed by other federal agencies—and that developed the Common Rule on institutional review boards for human experimentation.[41] At a minimum, any comparable rule for use of covered data in research should be adopted in consultation with them.

Despite promising elements, COPRA and USCDPA do not do enough to change the way data is collected and used today. Because purpose limitations are tied primarily to what is spelled out in a privacy policy, entities are still largely free to define what data they can collect. To guide legitimate collection, processing, and sharing purposes, normative boundaries need to move past privacy policies to more objective standards. COPRA and USCDPA each contain kernels of such principles: COPRA by defining a duty of loyalty and specifying which injuries constitute harmful data practices, and USCDPA by referencing what is "reasonably anticipated in the context of the covered entity's relationship with the individual." We recommend building on these and enlarging this foundation into a set of baseline duties toward individuals.

To guide legitimate collection, processing, and sharing purposes, normative boundaries need to move past privacy policies to more objective standards.

Our recommendation encompasses additional obligations under the duty of loyalty to take into the account the interests of individuals. Companies often refer to being "good stewards" of data. Indeed, a Google search of the term "good steward" with "privacy policy" turns up some 89,400 results, a large number of them corporate privacy policies that contain some version of "our commitment to be a good steward of your personal information." Stewardship implies a relationship of trust in which the steward looks out for the interests of the individuals linked to the data. An expanded duty of loyalty can make this aspiration concrete and enforceable.

We also believe the concept of "context" deserves recognition as a fundamental aspect of a privacy law. This is consistent with the Obama administration's proposed Consumer Privacy Bill of Rights—in which we (Kerry, Morris) had a hand—and also with other bills that allow for uses "consistent" with original purposes as well as the GDPR's allowance for "compatible use."[42] In a similar vein, the House Energy and Commerce draft lists purposes of processing that do not require affirmative consent because they are deemed "consistent with the context of the interaction between an individual and a covered entity."[43]

The concept of "context" deserves recognition as a fundamental aspect of a privacy law.

As technology philosopher Helen Nissenbaum has observed, "it is crucial to know the context—who is gathering the information, who is analyzing it, who is disseminating it and to whom, the nature of the information, the relationships among the various parties, and even larger institutional and social circumstances."[44] Context undoubtedly is difficult to pin down. But elevating the importance of this concept in a privacy law would loosen tethers to privacy policies or terms of consent and put the focus instead on the objective expectations and interests of individuals.

First, we suggest framing a baseline duty "to establish reasonable policies and practices to process and transfer covered data in a manner that respects the privacy of individuals." This duty would apply to all covered entities, including small and medium entities *(See Part III(A) of this report)*, but—in language that largely mirrors the data security provision in both USCDPA and COPRA—should be tailored to "the size and complexity of the covered entity and volume, nature, and intended uses of the covered data processed." The goal here is to establish a basic duty of covered entities to take individual privacy into account and take steps to protect it, but avoid being prescriptive about the implementation. For example, a neighborhood corner pharmacy should take reasonable steps to protect its customers' privacy, but what would be considered reasonable for its circumstances is likely to be very different from Google's.

In addition to this baseline duty, we suggest adding two elements to the overarching duty of loyalty provision. First, we would integrate the data minimization provisions of both COPRA and USCDPA into a duty to process and transfer covered data "only to the extent reasonably necessary, proportionate, and in accordance with law," and combine the exceptions to affirmative consent in COPRA and USCDPA into the following permitted use: "for purposes otherwise reasonably foreseeable within the context of the relationship between the covered entity and the individual." Including data minimization within the duty of loyalty affirms thoughtful collection, use, and transfer as a first principle.

The second element we recommend adding to the duty of loyalty is an obligation to communicate policies and practices for processing and transferring covered data "in a fair and transparent manner," also appropriate to the size and complexity of the covered entity and nature of data use, as well as "the context of the relationship between the covered entity and the individual." Fairness and transparency may be what COPRA Section 101(a) is getting at with its prohibition of "deceptive data practices." But it does not add to the statute or existing law, as it defines "deceptive data practices" only by violations of either COPRA, Section 5 of the FTC Act, or both. A general

duty of fairness and transparency may be implicit in the FTC Act, but it is helpful to make it more explicit as a foundation for provisions elsewhere and as a tool for the FTC to address manipulative communications with individuals, such as choice architecture labelled "dark patterns."[45]

Finally, we propose moving COPRA's articulation of harmful data practices (Section 101(b)(2)) into a "duty of care" provision—separate and distinct from the duty of loyalty. As discussed in connection with private right of action, the harms enumerated in COPRA Section 101(b)(2) are well-accepted in existing law. To conform more closely to the common law standards on which they are based and temper what might be interpreted as strict liability under COPRA, we would frame this branch as a duty not to process or transfer covered data "in a manner that reasonably foreseeably causes" the harms enumerated. Also to reflect common law, we suggest adding "highly" to COPRA's "offensive to a reasonable person"—the standard framed in Section 652 of the Second Restatement of Torts—when defining privacy intrusions that would constitute a harmful data practice.[46] In order to introduce context and underscore the objectivity of the standard, we would also add "unexpected" alongside "highly offensive," which is language also seen in the Data Care Act.

We would include in the duty of care an additional kind of harm, "discrimination in violation of the Federal anti-discrimination laws or the anti-discrimination laws of any State or political subdivision thereof applicable to the covered entity." Like other harms included in the duty of care, discrimination is well-established in existing law on remedies for discrimination. Framing the duty of care as separate and distinct helps to differentiate the standards of liability in our private right of action recommendation *(See Part I(B) of this report)* and links to the general duty of reasonable care underlying the law of negligence—rather than with the concept of fiduciary duties.

These recommendations embody our conception of baseline privacy regulation as a series of layers—an across-the-board baseline based on the duties of loyalty and care, coupled with a broad obligation to assess privacy risks and escalating prescriptive provisions as the scale of privacy risks and covered entities grows. They deliberately leave play in the joints, balancing flexibility and uncertainty and allowing for several different methods of application and iteration to fill in the gaps.

CONSENT AND SENSITIVE COVERED DATA

Members of Congress began their work on privacy with the recognition that the existing system of notice and consent places the burden on individuals to protect their information privacy, and they sought ways to shift this burden to the companies that collect and use the data. Despite widespread criticism of consent—the sheer number of consent requests alone places an unmanageable burden on individuals, rendering consent meaningless—it has proven to be a surprisingly durable legislative proposal.[47] Both COPRA and USCDPA call for "affirmative express consent" for both use and transfer of "sensitive covered data," with notable differences in how they define sensitive data and what exceptions they allow to consent. As discussed above, covered entities that obtain affirmative express consent would be exempt from several provisions of the two proposals, including data collection and minimization requirements.

In the abstract, we would prefer an approach that could avoid consent altogether. Nevertheless, we

accept that some use of individual consent has a role in baseline privacy legislation. Nearly every other legislative proposal incorporates consent requirements, and consent to use sensitive information resembles the GDPR requirement for "special categories" of data. It also responds to a commonly expressed desire on the part of the individuals to exercise control over personal data[48] and a conception of privacy as a right "to control, edit, manage, and delete information about [individuals] and decide when, how, and to what extent information is communicated to others."[49] On the other side of the coin, doing away with consent would require some categorical limits on the use of sensitive covered data that are difficult to define or apply. Thus, reliance on some individual choice accommodates a variety of interests, but our recommendations are informed by the premise that consent should be used as sparingly as possible to limit the number of consent requests individuals face.

COPRA and USCDPA both include in their definition of "sensitive data" categories such as precise location data, medical information, and others that are consistent with most proposals on the subject (Section 2(20) in both). COPRA, though, also considers metadata, all email addresses and telephone numbers, and "online activities" to be "sensitive data." These additions could sweep in so much data as to require affirmative express consent for almost everything. The effect would be to preclude some routine and innocuous uses and devalue the significance of consent, working against provisions to make consent more meaningful.

Even some of the terms defined as "sensitive data" in both COPRA and USCDPA will, in certain cases, not be sensitive at all, aggravating the risk of "consent fatigue" seen in the wake of GDPR. To address this concern somewhat, we propose an additional exception to affirmative express consent to carve out use cases where otherwise sensitive data (such as geolocation) is used briefly and then immediately discarded (such as an ephemeral response to a query for "what is the closest coffee shop"). An ephemeral use of location, for example, creates little risk if—as we propose—it "is not recorded or retained beyond the time strictly necessary to provide such immediate answer or service." This approach has the dual value of facilitating some innocuous uses of data and encouraging providers that *are* retaining location data in this kind of situation to cease the practice.

Both bills have provisions on what must be provided in notifications to individuals as a basis for affirmative express consent. Both would require such notification and affirmative express consent for any "material changes" to a privacy policy after initial collection or consent (Section 102(d) in both bills); in COPRA this is defined as one that "would weaken the privacy protection" applicable to the data affected. Here again, the bills could result in over-notification since, as drafted, they enlarge the underlying obligation for affirmative express consent beyond sensitive data.

We recommend narrowing this obligation by limiting notification to changes that "would be inconsistent with the terms on which an individual gave affirmative express consent to processing or transfer of sensitive collected data" or "would adversely affect the exercise of opt-out rights." This way, notice and consent to changes in privacy policies would correspond to the individual rights provided in legislation, rather than become a separate right that may have little relationship to individual expectations. It would also be consistent with provisions in both bills that limit transfers to third parties based on "reasonable expectations" of individuals.

In addition to controlling processing of sensitive information through consent, COPRA and USCDPA would provide individuals with an opportunity to "object" to, or opt out of, the transfer of other covered data to third parties. USCDPA has a bare bones provision (Section 104(d)) stating not much more than that, while COPRA (Section 105(b)) would give the FTC authority to delineate processes for individuals to do so, spelling out a number of requirements these processes should meet. We agree that people who prefer not to be tracked—or otherwise have data linked to them spread across information systems—should have ways to express their preference and have it respected. How to accomplish this is complicated technically and has cascading impacts through those ecosystems, making it an appropriate topic for rulemaking and spelling out factors to consider through legislation.

DATA SHARING (SERVICE PROVIDERS, THIRD PARTIES, AND DATA BROKERS)

In today's environment of business outsourcing, apps, and cloud services, many organizations rely on outside providers which also operate on and share such data in the context of marketing relationships and advertising networks. Many of these external relationships are important to online services and tools used by millions of Americans, and more broadly to the success of the information economy. At the same time, this essentially unlimited data sharing is at the root of much of the concern about privacy. Thus, it is vital to identify ways to enable appropriate data flows while protecting individuals against the almost unlimited recirculation of personal information that occurs today.

COPRA and USCDPA both address the sharing of covered information through provisions that cover "service providers" and "third parties," and specify how obligations applicable to covered entities apply when data is passed on to these other entities. USCDPA also has a provision targeted to data brokers—a specific type of third party—but COPRA does not. Senator Moran's CDPSA includes some helpful language about these external relationships. It expands the service provider provisions of COPRA and USCDPA by creating a specific section on service providers (Section 8) that has been carefully attuned to the differing relationships of these various interests. This can help minimize issues that have stalled bills, like data breach notification legislation, in the past. We therefore recommend that much of the substance of CDPSA's service provider section be worked into the service provider and third party provisions of legislation.

> Data sharing that has become essentially unlimited is at the root of much of the concern about privacy.

Service providers

Our recommendations for service providers draw from the work of all three of these proposals. The bills define a "service provider" as an entity that performs services or functions "at the direction of" a covered entity, and also define covered data transferred for these purposes as "service provider data." USCDPA adds a clarification that a service provider cannot be under either common ownership or control or common branding with the covered entity. COPRA adds another clarification that an entity handling covered data outside of a "direct relationship" with a covered entity is not treated as a service provider. Both clarifications should be included.

Because covered entities can exercise significant control over their service providers, USCDPA (Section 106) and COPRA (Section 203) spell out detailed obligations for service providers. Both do so in very similar terms: service providers cannot process service provider data except "on behalf of, and at the direction of" a covered entity, cannot transfer covered data to a third party without the covered entity obtaining affirmative express consent from individuals, and must delete or de-identity this data after completing the services. They exempt service providers from providing individual rights to access, correct, delete, or request portability with respect to service provider data, but require them to assist, to the extent practicable, in responding to such requests to covered entities.

The most significant additional service provider provision in CDPSA is an obligation for covered entities to enter into a binding contract with service providers. This contract requirement would be helpful in regulating relationships with service providers that have the leverage to set terms of service, leaving covered entities that want to negotiate privacy provisions in service contracts unable to do so. However, we do suggest that the description of what must be in a contract be more concrete, and that any contract should not "relieve a covered entity of any requirement or obligation with respect to such personal data that is imposed on the covered entity or service, as applicable, by this Act." The possibility that this provision might undermine contracts can be addressed by referring to obligations "directly" imposed; this would distinguish statutory requirements from obligations imposed by the required contracts. CDPSA also provides more guidance than USCDPA or COPRA in spelling out the extent of service provider duties to respond to individual control requests.

Another subject CDPSA uniquely addresses is obligations for service providers to give notice to covered entities of events affecting processing of service provider data. These cover processing for legal requirements such as lawful government access requests or litigation, changes to policies or practices affecting contract compliance, and subcontracting any part of processing service provider data. The latter would give the covered entity an opportunity to object; concerns about this limiting discretion could be addressed with contract language, such as a provision that an objection "shall not be interposed arbitrarily." A service provider should have the same obligation of due diligence that a covered entity has when transferring service provider data, in addition to the obligation to have a contract in place.

Third parties

Our proposals for third parties also draw from USCDPA, COPRA, and CPDSA. Under COPRA and USCDPA, a "third party" is an entity that processes data transferred from a covered entity, is not a "service provider," and is not under either common ownership or control or common branding with the covered entity. COPRA and USCDPA also regulate third parties in similar ways. Both COPRA and USCDPA prohibit third parties from processing data in a manner that is "inconsistent with the reasonable expectations" of affected individuals. However, they effectively allow third parties to transfer sensitive covered data, provided the individual's affirmative express consent to the covered entity allows for such transfer. The provisions explicitly recognize that the third party is permitted to rely reasonably on the representations of the covered entity with regard to these expectations, but COPRA adds a requirement that the third party exercise reasonable due diligence with respect to these representations and find them credible.

These limitations make sense. After all, the covered entity has the primary relationship with the individuals linked to the data and thus is better positioned to make judgments about their expectations. Even so, if the covered entity's publicly available privacy policies declare unequivocally that it will not share certain data with third parties, a third party should be on notice. Based on language adapted above from USCDPA, we suggest using "reasonably foreseeable in the context in which the [data being shared] was collected or processed prior to transfer" in place of "reasonable expectations." We also would add to the list purposes that are inconsistent with (a) an individual's grant of affirmative consent or exercise of opt-out rights, or (b) practices and policies identified in notices and disclosure statements *(See Part IV(C) of this report)* on the basis that these uses are per se inconsistent with context or reasonable expectations. In addition, the list could bar any other purposes that would violate privacy legislation or other federal law.

These duties could be reinforced by building on the CDPSA proposed duties for covered entities to conduct due diligence in vetting service providers and investigating their compliance with obligations. Accordingly, we propose adding a general duty for covered entities to exercise "reasonable due diligence" in selecting service providers and choosing to transfer data to third parties, and "reasonable oversight" of their compliance with legislative requirements. This encapsulates both "reasonable due diligence" called for in the USCDPA and COPRA third party provisions and the more detailed language in the CDPSA service provider provision and expands their application to third parties. Due diligence and oversight would help ensure that companies consider, for example, how their website configuration shares data, what data brokers they share with, or how software developer kits and APIs are employed. As with other general duties we recommend, this should be "appropriate to the size and complexity of the covered entity; the volume and uses of the covered data subject to transfer; and the risk of harm to individuals that may result from the disclosure of such data."

As of 2013, there were an estimated 3,500 to 4,000 data brokers in the data broker industry.

Data brokers

Section 203 of USCDPA would require data brokers to register with the FTC and pay a $100 registration fee. In addition to contact information, the registration statement would include "any additional information the data broker chooses to provide concerning its data collection and processing practices," and the FTC would be required to publish a list of registered data brokers on its website. Senator Wicker is right in including a separate provision on data brokers. While data brokers may well be covered as third parties or service providers, they present additional issues of their own. They operate as data aggregators, combining transferred personal information from many sources with additional publicly-available information such as property registries, motor vehicle registrations, and voting lists. This aggregation of data adds enormously to the granularity of information available online; for example, until 2019, Facebook partnered with data brokers to enhance the precision of ad targeting on its platform.[50] In addition, data brokers often collect this data secondhand, so their existence and identity are usually unknown to the individuals linked to the data they hold. The Equifax data breach brought home to many Americans the impact that can come from companies they never dealt with directly.

As of 2013, there were an estimated 3,500 to 4,000 data brokers in the data broker industry.[51] Many of these take care in the provenance of the data they acquire and handle it with caution for the privacy of individuals, but some do not. It is possible, for example, to acquire lists of individuals identified as having sexually transmitted diseases; there may be appropriate uses for such information but there are far more potentially inappropriate uses. In response to a 2012 FTC inquiry, a number of data brokers established portals by which individuals could see what data pertaining to them the brokers had—voluntary precursors to rights of access under GDPR, CCPA, and—potentially—federal privacy legislation.[52]

The USCDPA data broker provision is a good start, but should do more to address issues specific to data brokers. As covered entities, data brokers would be subject to various provisions including individual rights, but federal legislation can do more to enhance transparency about data aggregation practices that are out of public view. The information submitted with a broker's registration statement could be significantly more informative by including more ways to reach the broker, its privacy disclosures, the categories of information it processes about individuals, and links to portals to exercise individual rights. In addition, we recommend—consistent with Senator Ron Wyden's (D-OR) Consumer Data Protection Act of 2018—that a data broker provision include a requirement for the FTC to develop an API or other mechanism to permit individuals to exercise their individual rights without having to track down and make a request to every single data broker that has collected data linked to them.[53]

The costs of developing and maintaining such a mechanism could be funded by fees and penalties paid under the provision. A registration fee of $100 is a small sum for many data brokers, and it should be scaled according to number of individuals linked to the data (we suggest $100 per 1,000 people). Likewise, a penalty of $50 per day for failure to register seems low; $100 might strike a balance or the penalty could be scaled depending on the number of individuals involved or the length of the late period.

We also suggest clarifying the definitions of "service provider" in COPRA and USCDPA to ensure that data brokers cannot benefit from compliance exemptions better suited for service providers. Data brokers may receive covered data as "service provider data" in the course of performing services for a covered entity, but they also may receive covered data as part of their business of data aggregation. We suggest excluding data brokers from the definition of "service provider" to the extent that the data broker "transfers covered data to a covered entity or processes service provider data based on or in combination with covered data under the control of such data broker."

Table 4: Obligations of Service Providers and Third Parties
Different obligations apply based on differences in control over transferred covered data.

Service Providers	Third Parties
Limits on Processing: Service providers should not process data for any purpose other than that performed on behalf of a covered entity, as provided in legislation, or pursuant to a contract.	**Limits on Processing:** Third parties should not process data in a manner that is inconsistent with an individual's consent to the transfer of sensitive data, opt-out rights, reasonable expectations, covered entity's notice and transparency provisions, or applicable law.
Data Transfer: Service providers should not transfer data to a third party without the affirmative express consent of the individual.	**Data Transfer:** If covered entities transfer data to a third party, the third party should be able to rely on the covered entity's representation regarding the expectations of related individuals, providing the third party conducts reasonable due diligence.
Notification: Service providers should notify the covered entity of any amendments to privacy policies and practices, legal obligations to provide data (e.g., a subpoena), or intent to employ a subcontractor to collect or process data.	
Right to Control: When covered entities fulfill individual requests for the right to control and right to recourse, service providers should provide appropriate support, and should respond to requests from a covered entity for deletion, de-identification, correction, or portability of service provider data.	
Exemption: Service providers should be exempt from certain obligations, like duty of loyalty, duty of care, basic privacy statements, right to control, right to recourse, and affirmative express consent provisions, but should otherwise share the same obligations as covered entities.	**Exemption:** Third parties should be exempt from the duty of loyalty but should otherwise share the same obligations as covered entities.

B. Civil Rights

DATA DISCRIMINATION AS A CIVIL RIGHTS ISSUE

The collection, processing, and sharing of personal information has become a significant civil rights issue in response to advances in predictive analytics, big data, and machine learning. In 2014, a White House task force conducted a study of the effects of big data on society, the economy, and governance and found that "while big data can be used for great social good, it can also be used in ways that perpetuate social harms or render outcomes that have inequitable impacts, even when discrimination is not intended."[54] In the wake of that report, both the White House and Federal Trade Commission conducted further inquiries into the potential for discrimination in data science and ways to avoid the misuse of data.[55]

These concerns have only increased with the quickening pace of machine learning and artificial intelligence (AI). In February, we (Kerry) wrote that

"as artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed."[56] In turn, analytical tools can replicate inequities and discrimination embedded in training data, mask false correlations or overfit to data, and exhibit other flaws that can affect disadvantaged groups.

Systemic bias can occur as a result of human design error, selection of training data, or validation of results. Systems can also generate hidden proxies for legally protected characteristics, such as location for race or income.

Systemic bias can occur as a result of human design error, selection of training data, or validation of results. Systems can also generate hidden proxies for legally protected characteristics, such as location for race or income.[57] This concern is especially salient in certain contexts, such as policing and criminal justice, because of their impact on people's lives and a history of disproportionate consequences on disadvantaged groups.[58] But it also bears on more subtle impacts in the commercial arena where hidden proxies can reduce opportunities for members of disadvantaged groups. In a stark example, Latanya Sweeney, a Harvard professor and former FTC chief technology officer, demonstrated that Google searches using names associated with African Americans were more likely to generate advertisements relating to arrest records and less favorable credit cards.[59]

The issue presents three primary challenges for privacy legislation. The first is how civil rights fit into privacy legislation. There is a body of existing anti-discrimination laws and jurisprudence, and specialized enforcement agencies like the Equal Employment Opportunity Commission (EEOC) have decades of experience in the field. The existing statutes, such as Title VII of the Civil Rights Act or the Americans with Disabilities Act, are outside the experience and mandate of the FTC.[60] Meanwhile, discrimination presents novel issues in the information privacy context. These circumstances raise questions as to what a non-discrimination provision in a privacy statute can add to existing law—and to what extent it should.

These questions add to a second challenge: the charged politics that surround civil rights. Any enlargement or contraction of existing rights and remedies cuts across polarized social issues that are subjects of electoral trench warfare and beyond the effective reach of privacy legislation. This is especially the case for anything that enlarges categories of individuals protected under federal law. Developments that may take several election cycles or long-term social change to resolve (as we saw with same-sex marriage) make a civil rights provision heavy cargo for privacy legislation to carry through Congress.

The weight of this cargo is magnified by the number of congressional committees tasked with oversight of civil rights laws. In the Senate, these consist primarily of the Judiciary Committee, Banking, Housing, and Urban Affairs Committee, and Health, Education, Labor, and Pensions Committee—but not the Commerce, Science, and Transportation Committee that oversees the FTC and is the key committee on privacy legislation. Congressional committees guard their jurisdiction jealously, and Metcalfe's law applies

here: the complexity of the path forward increases exponentially with the number of nodes it touches.

The third challenge is the algorithms themselves. They are complex and opaque, and machine learning development is outpacing human understanding. Numerous studies, analyses, and ethical frameworks have identified risks and benefits of AI and propounded various practices to mitigate erroneous, discriminatory, or otherwise undesirable outcomes of algorithmic predictions and decisions.[61] Even so, a generally applicable prescription for preventing and identifying algorithmic discrimination is a work in progress.

These challenges counsel against overreach but not for sidestepping discrimination issues altogether. We (Kerry) wrote that "[u]se of personal information about [attributes such as skin color, sexual identity, and national origin], either explicitly or—more likely and less obviously—via proxies, for automated decision-making that is against the interests of the individual involved thus implicates privacy interests in controlling how information is used."[62] This makes discriminatory use of covered data an appropriate subject for federal privacy legislation. Seen in relation to the use of personal information, the pertinent injury is not the discrimination as such, but the use of personal information in ways that are against the interests or contextual expectations of the individual linked to that information. As such, anti-discrimination fits into the fundamental conceptual framework that underlies our recommended duties of loyalty and care *(See Part II(A) of this report)*.

Algorithms create a sharp genetic mutation in how discrimination can occur and thus in how it can be detected and regulated. The type of discrimination considered under the Civil Rights Act of 1964 and its progeny envisioned human agency—decisions made by proprietors, personnel officers, landlords, and other individuals.[63] But in the 21st century, decisions can be made by machines or software—without a human in the loop.[64] Machines should not have a license to discriminate where humans cannot. Yet reconstructing the basis for these decisions is a difficult undertaking of a different order from traditional employment or housing discrimination cases. This difficult task requires new tools, which legislation can provide by governing the collection, processing, and sharing of personal information.

> Machines should not have a license to discriminate where humans cannot.

CIVIL RIGHTS IN COPRA AND USCDPA

COPRA and USCDPA show some level of bipartisanship on the issue of algorithmic discrimination. They agree that it has a place in privacy legislation, and that the FTC should conduct a study of the discriminatory use of algorithms. They differ, though, on the roles of the legislation and the FTC in addressing such discrimination.

USCDPA (Section 201) provides for an indirect role, with the FTC to "endeavor" to refer "information that any covered entity may have processed or transferred covered data in violation of Federal anti-discrimination laws" to relevant federal or state agencies authorized to enforce these laws, and to cooperate with these agencies.

COPRA (Section 108) makes discrimination a violation of the FTC Act by declaring:

> *A covered entity shall not process or transfer data on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability ....*

in any way that "unlawfully discriminates against or otherwise makes the opportunity unavailable" in housing, employment, credit, or education, or that "unlawfully segregates, discriminates against, or otherwise makes unavailable" any public accommodation.

This language, incorporating a legislative proposal by Free Press and the Lawyers' Committee for Civil Rights Under Law,[65] substantially tracks the Title VII of the Civil Rights Act of 1964. The phrase "on the basis of" draws from the Free Press and Lawyers' Committee's public accommodation provision, while Title VII prohibits employment discrimination "because of" protected characteristics.[66] Most of the protected categories in COPRA are the subject of existing federal anti-discrimination laws, although COPRA omits age. Some categories in COPRA, though, are not covered by existing laws. "Biometric information," as defined in COPRA, includes genetic data covered by the Genetic Information Nondiscrimination Act, but the term also encompasses other characteristics not covered by existing laws.[67] Familial status is currently protected only in the context of housing under the Fair Housing Act.[68] Sexual orientation is not explicitly covered by federal statutes, although it is by jurisprudence, EEOC interpretation, and executive order addressing discrimination within the federal government.[69] Gender identity remains a matter of litigation and debate.[70]

We see the two proposals as consistent with the concerns about algorithmic discrimination and challenges that we discuss above. USCDPA reflects that the primary authority and expertise for enforcement of federal anti-discrimination laws rests with the agencies designated by those laws. It is possible to both maintain the role of the EEOC and other federal agencies and make discriminatory uses of data a violation of privacy law and the FTC Act, as COPRA proposes. With this authority, the FTC can play an adjunct role in non-discrimination enforcement, bringing to bear expertise in technology, data, and algorithm use it has developed over the past decade.

Thus, we recommend combining elements of both bills by including a version of COPRA's anti-discrimination provision as well as USCDPA's provision on FTC referrals to other agencies. This would maintain the primary role of existing enforcement agencies, while giving the FTC authority to act as a force multiplier and to inform understanding of algorithms and their effects. Such anti-discrimination provisions also would flesh out the provision in our proposed general duty of care that prohibits discrimination in ways that violate anti-discrimination laws. Under a privacy statute, the gravamen of a violation would not be the discrimination as such, but the use of covered data in ways that are harmful to an individual.

We also suggest changes to the COPRA anti-discrimination language to address how algorithmic discrimination differs from that prohibited by current federal non-discrimination statutes and to hew more closely to current and future federal laws. Instead of using "on the basis of" protected classifications, like COPRA and the Free Press and Lawyers' Committee, we propose the provision should prohibit data processing or transfer "that differentiates an individual or class of individuals." This language adapts to changes in the nature of decision-making

by shifting the focus from the decision to the output of an algorithm.

Further, we suggest that the provision apply to differentiation "with respect to any category or classification protected under the Constitution or law of the United States as they may be construed or amended from time to time" rather than enumerate specific protected classes. Besides mirroring our recommended duty of care language, this change accomplishes two things. It avoids limiting protected categories to those mentioned in the statute—under a canon of statutory construction, courts treat statutory references to existing laws as the laws in effect at the time of enactment unless there is specific language to indicate otherwise. In addition, it sidesteps debate about what categories should or should not be included in privacy legislation, leaving resolution of these questions to ongoing legislative, judicial, and political debate.

We also recommend importing, in a modified form, a provision from the House Energy and Commerce Committee draft that would provide a fuller airing of the workings of contested algorithms: a disparate impact provision entitled "burden of proof" (Section 11(c)). It provides:

> *If the processing of covered information … causes a disparate impact on the basis of any characteristics [protected under previous provisions], the covered entity shall have the burden of demonstrating that—*
>
> *(A) such processing of data—*
>
> *(i) is not intentionally discriminatory; and*
>
> *(ii) is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; and*
>
> *(B) there is no reasonable alternative policy or practice that could serve the interest described in clause (ii) of subparagraph (A) with a less discriminatory effect.*

This provision is modeled on the Civil Rights Act of 1991 which, like other civil rights legislation discussed above, is a product of pre-digital times when issues more directly involved the intent of people and the organizations they acted for.[71] To focus on algorithms instead, we suggest replacing "causes a disparate impact on the basis of" with the language we suggested earlier: "differentiates an individual or class of individuals with respect to any category or classification protected under the Constitution or law of the United States."

If algorithms or artificial intelligence exercise significant control with limited human oversight, familiar methods of gauging intentionality fit poorly.

The rebuttal showing should be adapted to algorithms as well. If algorithms or artificial intelligence exercise significant control with limited human oversight, familiar methods of gauging intentionality fit poorly. In this context, an "intentionally discriminatory" standard has uncertain meaning. Instead, to reflect that the inquiry is focused on data analytics, we propose requiring the covered entity to demonstrate that its data processing is "independent of any protected characteristic or classification." Nor does "policy or practice" really fit algorithmic decision-making, even though algorithms may have policies or practices embedded in certain instructions; thus we suggest replacing this provision with "there is no reasonable method of processing" to serve the same legitimate, nondiscriminatory interests.

We recognize that the use of disparate impact tests remains contested; for example, a recently proposed Department of Housing and Urban Development rule could make it more difficult to prove disparate impact under the Fair Housing Act.[72] But when algorithms result in disparate impact, it is appropriate to shift the burden of proof to the party that employs or operates the algorithmic decision-making system. Such burden-shifting mechanisms rest significantly on the superior control of and access to information of the employer or other party assigned the burden.[73] This information disparity is overwhelmingly and uniformly the case for any algorithmic decision-making. Moreover, a rebuttal standard is a necessary corollary to shift focus from human decision-making to algorithms by making the prima facie showing based on "differentiating". This is, in effect, a disparate impact showing, and without the rebuttal standard, the disparate impact prima facie test could become per se discrimination.

"The algorithm did it" should not be a sufficient defense in a discrimination case.

Without this burden-shifting, a black box could provide impunity, encouraging willful ignorance on the part of covered entities that employ algorithmic decision-making. This would work against an array of recommended practices for ethical and responsible use of algorithmic decision-making and accountability. "The algorithm did it" should not be a sufficient defense in a discrimination case.

C. Algorithmic Decision-Making

The risk of discrimination addressed in the preceding section of this report looms large in algorithmic decision-making. However, algorithmic decision-making can potentially result in adverse effects on individuals that fall outside the context of civil rights laws. We (Kerry) have described these effects: "As artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed."[74]

That report examined several ways to address algorithmic decision-making in privacy legislation. In general, these are: (1) addressing discriminatory outcomes directly; (2) indirectly mitigating discrimination by regulating processing of personal information; and (3) requiring accountability and transparency in uses of algorithmic decision-making to help prevent and identify discriminatory outcomes. COPRA and USCDPA reflect all three categories in varying degrees—the first category in their references to federal civil rights law; the second through generally applicable data collection, processing, and sharing requirements; and the third through algorithmic or privacy impact assessment provisions. We focus on the latter in this section of the report.

COPRA (Section 108) requires annual "algorithmic decision-making impact assessment[s]" if (1) a covered entity engages or assists others in algorithmic decision-making and (2) the algorithmic decision-making system is used to advertise housing, education, employment, credit, or access to public accommodations. Such an assessment must evaluate the design and data used to develop the algorithms, describe the testing for accuracy,

fairness, bias, and discrimination, and assess whether the algorithms discriminate on the basis of listed characteristics *(See Part II(B) of this report)*. A covered entity may optionally use an outside auditor and must make its assessment available to the FTC upon request. The FTC, in turn, is directed to publish a report on algorithm use and civil rights every three years after enactment.

USCDPA (Section 201) has a parallel provision on "algorithm bias, detection, and mitigation," which is contained within its Title II on "data transparency, integrity, and security" but frames an alternative to the COPRA civil rights provision. USCDPA calls for the FTC to issue "algorithm transparency reports" that examine "the use of algorithms to process covered data in a manner that may violate Federal anti-discrimination laws," and to develop guidance on "avoiding discriminatory use of algorithms."

Each bill also has a section on a related tool: privacy assessments. USCDPA (Section 107) requires "privacy impact assessments" only for "large data holders" (which it defines as entities that process covered data from more than five million individuals or devices, or sensitive covered data from more than 100,000 individuals or devices). COPRA (Section 202) requires all covered entities, except for small businesses, to appoint privacy and security officers who would be responsible for conducting annual "privacy and data security risk assessments."

An algorithmic decision-making provision can help covered entities consider how their data collection and processing affect individuals. Therefore, we recommend combining elements of both COPRA and USCDPA into a standalone provision on algorithmic decision-making—with a more narrow applicability than COPRA but broader content than either bill—and linking this provision to other accountability requirements.

Algorithmic impact assessments are vital tools to support civil rights in the context of personal data processing, but they should consider broader harms than those covered by federal anti-discrimination laws.

We suggest two realignments in the organization of an algorithmic decision-making section. Although USCDPA (Section 201) and COPRA (Section 108) address algorithms as an adjunct of discrimination enforcement, we first suggest isolating the two topics into separate sections. Second, we agree with USCDPA's approach in categorizing algorithmic decision-making in the Title II "data transparency, integrity, and security" section—rather than in the Title I "individual consumer data rights" section—but we recommend all obligations for covered entities belong in Title II. Covering algorithmic decision-making under the Title II heading of responsibilities and oversight would be consistent with a shift in regulatory paradigm toward greater emphasis on how covered entities handle data and would group this provision among others aimed at improving internal and external accountability. As we later discuss, organizational accountability is essential to privacy and data protection and appropriately-scaled accountability measures for algorithmic decision-making are necessary *(See Part III(C) of this report)*.

Putting algorithmic decision-making in its own section would de-link algorithmic transparency and accountability from civil rights. Algorithmic impact assessments are vital tools to support civil rights in the context of personal data processing, but they should consider broader harms than those covered by anti-discrimination laws. In turn, a record of

algorithmic impact assessments and FTC reports can inform future debate about forms of discrimination and the broader risks or benefits of algorithmic decision-making.

Third, consistent with our recurring recommendation to scale obligations according to risk and scale, we suggest that algorithmic decision-making impact assessments only be mandatory for large data holders. Large data holders are most likely to use algorithmic decision-making at a scale and complexity that can affect many people, and an algorithmic impact assessment can amount to a significant or complex regulatory requirement. Targeting algorithmic decision-making impact assessments to large data holders would not entirely free smaller entities from all responsibility for the effects of their algorithms because, as we conceive it, all covered entities would still be subject to the duties of loyalty and care (which would mandate non-discrimination) and to a baseline obligation to conduct privacy risk assessments.

Fourth, we recommend broadening the scope of algorithmic decision-making impact assessments for large data holders to include both an initial risk assessment prior to deploying algorithmic decision-making and annual audits of the results after deployment. Both COPRA and USCDPA prescribe their respective obligations for algorithmic decision-making impact assessments or privacy risk assessments annually. The effect would be that most entities would conduct assessments after-the-fact alongside whatever other algorithmic decision-making they deploy over the course of the year. Because advance thought on the impact of algorithmic decision-making can help avoid undesirable outcomes, we recommend requiring large data holders to conduct impact assessments when "considering" using a new algorithmic decision-making system. For algorithmic decision-making systems operating prior to enactment of federal privacy legislation, large data holders should conduct impact assessments within one year of the law's enactment.

Fifth, we suggest broadening the types of algorithmic decisions covered. COPRA lists only five specific categories: housing, education, employment, credit, and public accommodations. All of these can clearly have a major impact on people's lives and would fit within the GDPR's provisions on "automated individual decision-making" that "produces legal effects or … similarly significantly affects [an individual]," but are not the only effects of that type.[75] To protect individuals and enlarge understanding of the impact of algorithmic decision-making, however, we believe the trigger to conduct algorithmic decision-making impact assessments should be when covered entities consider using systems that more broadly "may have a significant effect on individuals," which is similar to GDPR.

We recognize that this begs the question as to what "significant" effects entail. The answer effectively lies in the baseline privacy risk assessment applicable to all covered entities—if the necessary consideration of "the adverse consequences … to individuals and their privacy" suggests there may be significant effects, then a full algorithmic impact assessment may be in order for large data holders. Furthermore, the information gained from such privacy risk assessments and algorithmic decision-making impact assessments in the aggregate could help inform understanding of this question over time.

Here, we also borrow loosely from Senator Wyden's Algorithmic Accountability Act of 2019 (AAA), which defines "high-risk automated decision system" as one that "poses a significant risk" to individual privacy or security of individuals and makes decisions

regarding "sensitive aspects of [individuals'] lives."[76] Housing, education, employment, credit, and access to public accommodations provide concrete examples of "significant effects," but this list is not exhaustive. We also suggest looking to AAA when specifying the scope of an algorithmic decision-making impact assessment. COPRA requires algorithmic decision-making impact assessments to evaluate (a) the design and training data underlying the system, (b) evaluation of accuracy and fairness, and (c) discriminatory results. We also recommend that algorithmic decision-making impact assessments include a cost-benefit analysis—a provision from AAA—but suggest abbreviating it consistent with our scaled approach: "an assessment of the relative benefits and costs of the algorithmic decision-making system in light of the nature of the covered data used, the accuracy and fairness, the relative risk of error bias or discrimination, and the impact on individuals and other affected interests."

Like COPRA, we recommend that covered entities should be required to conduct these assessments annually. Such annual assessments operate as an ongoing check against unlawful discriminatory impacts and provide a factual record from which to assess the broad effects of algorithmic decision-making.

Both COPRA and USCDPA define algorithms, for purposes of addressing decision-making, to include a computational process that "facilitates" human decision-making. Because "facilitates" is a broad term that could encompass the relatively simple and human-driven computations of a spreadsheet, we suggest a modification along the lines of providing "significant support" for human decision-making instead.

Both COPRA and USCDPA call for the FTC to publish a report on algorithmic decision-making within three years of enactment, but in different ways. USCDPA calls on the FTC to report "on the use of algorithms to process covered data in a manner that may violate Federal anti-discrimination laws;" COPRA broadens the scope to "the use of algorithms and benefits, costs, and impacts described in this section." Because the implications of algorithmic decision-making go beyond discrimination and federal anti-discrimination law, we prefer the latter language.

By including algorithmic decision-making with other Title II accountability provisions and requiring impact assessments for large data holders, we aim to make more concrete the stewardship and trust that we see as a central goal of information privacy legislation.

By including algorithmic decision-making with other Title II accountability provisions and requiring impact assessments for large data holders, we aim to make more concrete the stewardship and trust that we see as a central goal of information privacy legislation.

Part III — The Solvable Issues

KEY RECOMMENDATIONS

- The scope of "covered entities" should reflect the jurisdiction of the Federal Trade Commission Act but also allow the FTC to enforce privacy compliance with respect to common carriers and nonprofits. This will require adapting the definition of "small business" to address nonprofits; the FTC should conduct a rulemaking to determine thresholds for this sector.
- There should be no wholesale exception for small entities from federal privacy legislation because such entities can cause serious privacy harm (Cambridge Analytica as one example). Instead, small and medium entities should be exempted from certain process obligations like data access, correction, deletion, and portability, as well as our proposed right to recourse.
- COPRA has an "executive responsibility" provision (Section 201) which requires executive-level officers to certify the covered entity maintains adequate internal privacy controls and reporting structures. We recommend moving this certification provision to a section on transparency and detailed disclosures, while limiting certification requirements to large data holders. We also suggest raising the threshold for "large data holders" to organizations that process or transfer covered data of 30 million individuals, households, or devices, or sensitive covered data of 3 million individuals, households, or devices.
- Data security is an essential element of privacy protection, and COPRA (Section 107) and USCDPA (Section 204) have sound data security provisions. To flesh out these provisions, FTC guidance is preferable to rulemaking because it is more agile in the fast-changing and technical area of cybersecurity.
- All organizations should be responsible for conducting privacy risk assessments, tailored to the scale of the covered entity, covered data, and privacy risks. Privacy risk assessments should be a specific and separate organizational accountability requirement.
- We recommend dividing COPRA's requirement for privacy and security officers and comprehensive written privacy and security programs (Section 202) into two separate subsections. These, along with USCDPA specifications for risk assessments by large data holders, should become additional requirements for organizational accountability.

A. Covered Entities

SCOPE OF COVERAGE

Like most privacy bills, COPRA (Section 2(9)) and USCDPA (Section 2(8)) use the term "covered entities" to define which entities are subject to the legislation.

USCDPA defines "covered entity" as any entity that "operates in interstate or foreign commerce," which is the broadest possible reach for a federal economic statute. Meanwhile, COPRA proposes a narrower definition—any entity subject to the Federal Trade Commission Act that processes or transfers covered data—but maintains or adds exclusions for various sectors. Since the FTC has jurisdiction over much of interstate commerce, the COPRA definition covers much of the same expanse as does USCDPA. Nevertheless, there are some sectors carved out from FTC jurisdiction, most notably banks and savings and loan institutions, which other agencies and privacy statutes regulate. A separate savings provision in Section 404 of USCDPA preserves these and other laws—so it may be functionally similar in scope to COPRA—but USCDPA's broad definition of covered entities does raise questions as to its applicability to sectors regulated under other statutes.

We think using the FTC Act as a jurisdictional baseline covers enough without covering too much. With the addition of jurisdiction over common carriers and nonprofits, as discussed next, the FTC would have broad authority to cover much of the U.S. economy without running up against existing federal statutes and, with those, additional affected industries and congressional committees of jurisdiction.

COMMON CARRIERS AND NONPROFIT ORGANIZATIONS

USCDPA would include within the scope of covered entities two types of entities not normally covered by FTC Act, common carriers—which include traditional wireline and wireless telephone carriers—and nonprofit organizations. Some nonprofits process personal data on a large scale—for example, colleges and universities are subject to FERPA only when it comes to their own students, but not when they collect data on high school students to recruit applicants.[77] In addition, some large insurance companies and medical providers also operate as nonprofits.

> It makes little sense for comparable entities that collect the much of the same kinds of data to be subject to different rules.

Most legislative proposals sweep in common carriers and nonprofits with respect to a federal privacy statute, but COPRA does not. It is not clear why. It is possible the common carrier omission is related to some hope that the repealed 2015 Open Internet Order can be reinstated and, with it, some form of the broadband privacy rules that were overruled by Congress in 2017.[78]

For reasons of both substance and strategy, we consider it logical to include FTC jurisdiction over common carriers for purposes of privacy enforcement. As common carriers like AT&T and Verizon increasingly shift from mainly providing network infrastructure to also providing media and other internet services, there is little to distinguish them from information services like NBC Universal, Apple,

or ViacomCBS. It makes little sense for comparable entities that collect the much of the same kinds of data to be subject to different rules.[79]

More importantly, it is in the interest of individuals to interact with one set of rules that provide some trust that—regardless of the type of business or service they choose—personal data will be handled in ways consistent with individual expectations and interests. Baseline privacy legislation cannot rationalize all of the fragmentation that individuals face when it comes to privacy rules, but the common carrier exemption is one anomaly that is within easy reach of privacy legislation under the jurisdiction of the Senate and House Commerce Committees.

A wholesale exception could be a license for mischief. Some of the most notorious privacy failures have come from entities that would have qualified as small businesses.

One clear indicator that the privacy debate is more promising now than in the past was when—two years ago—traditional communications carriers, internet service providers, and edge providers began urging comprehensive privacy legislation and speaking in similar terms about making it competitively and technologically neutral. Before that, battles over the FCC's 2017 broadband privacy rules—ensuing from the agency's 2015 Open Internet Order—helped block federal privacy legislation, as traditional common carriers subject to communications privacy laws, ISPs subject to the new broadband privacy rules, and largely-unregulated edge providers fought over competitive advantages.[80]

Passing legislation requires piecing together coalitions that build support and neutralize opposition. This union of past adversaries—who are no longer working to block legislation—is a force multiplier and including common carriers grows the coalition.

SMALL BUSINESS EXCEPTION

COPRA entirely excludes "small businesses" from the legislation. Both Section 2(23) of COPRA and Section 2(23) of USCDPA define "small business" using the same benchmarks: entities with an annual gross revenue not greater than $25 million over the previous three-year period, that process covered data from less than 100,000 individuals, and derive less than 50 percent of their revenue from transferring covered data. In COPRA, though, covered entities must meet all three benchmarks to qualify, while in USCDPA, they only need to meet at least one. On the other hand, USCDPA does not broadly exclude small businesses from all privacy requirements—only from the Section 103 provisions on individual rights of control and Section 105 limits on collection, processing, and retention of covered data.

Creating some exceptions for small businesses recognizes that there is a regulatory burden in complying with privacy laws. It takes time, personnel, resources, and considerable back-end engineering to design systems for consent, exercise of individual rights, and controls on data. In fact, IAPP and Ernst and Young estimated that Fortune 500 companies could spend almost $8 billion collectively to prepare for GDPR compliance, and an initial regulatory impact assessment for the California Attorney General's office estimated that CCPA initial compliance costs could total up to $55 billion.[81]

Nevertheless, a wholesale exception could be a license for mischief. Some of the most notorious

privacy failures have come from startups that began as small businesses—Cambridge Analytica, for a prominent example, or Brightest Flashlight, a smartphone app that collected continuous geolocation information without adequate disclosure.[82] Indeed, many of the cases tagged with "privacy and security + consumer privacy + data security + identity theft" on the FTC's website relate to small businesses.[83]

Accordingly, we recommend retaining a small business exception, but limiting its applicability to specific provisions. It should be noted that if nonprofit organizations are included in the scope of legislation, then the name for "small business" provisions would need to change and some benchmarks for nonprofits would need to be added. For this reason, we refer to "small and medium entities" (SMEs) instead of "small businesses" in this report. We have not identified any comparable benchmarks for the nonprofit sector, so we suggest the FTC be given rulemaking authority to establish the appropriate benchmarks for "small or medium entities" with regards to nonprofits, with the proviso that nonprofits that process data of less than 100,000 individuals, households, or devices automatically qualify—as it would be anomalous for small nonprofits to face privacy obligations that their for-profit counterparts do not.

As discussed earlier, we propose that SMEs be exempt from obligations that require significant business process engineering (e.g., the rights of access, correction, deletion, portability, and recourse) or that are more prescriptive (e.g., appointment of privacy and security officers and written privacy and security assessments). But a wholesale exception from a privacy law does not make sense. Some provisions, like data minimization requirements, should apply to all covered entities—the example of Cambridge Analytica's lack of boundaries to collect, process, and retain data provides a powerful case in point.

We think the better approach is to include baseline duties that both apply to all covered entities across the board but are also flexible according to the scale of the covered entity and the privacy risks. We discuss these requirements in the previous sections on duties of loyalty and care and other limits on processing *(See Part II(A) of this report)*. Below, we discuss additional basic provisions for all covered entities—data security requirements—as well as graduated obligations for larger covered entities.

> Information about people is not private if entities who shouldn't have access to it can steal it.

B. Data Security

Data security has been an element of privacy and data protection since the first fair information practice principles were propounded early in the mainframe computing era, for one simple reason: information about people is not private if entities that shouldn't have access to it can steal it.[84] Data security is included in CCPA and GDPR, and a number of states have adopted data security laws that set out basic practices such as access controls and training.

The latter come on top of state data breach notification laws. Between 2003—when California became the first state to adopt a data breach notification law—and 2018, all 50 states plus the District of Columbia have adopted versions of such laws. In 2003, Senator Dianne Feinstein (D-CA) introduced a federal data breach notification law—the first of numerous bills seeking to standardize differing notification requirements across the United States—but

to date, no federal data breach notification law has yet been enacted.[85] In 2015, President Obama called for enactment of the Personal Data Notification and Protection Act in his State of the Union speech, and there were serious efforts to enact that bill and others.[86] However, these efforts foundered over impasses on federal preemption and the potential impact on breach liabilities among retailers, banks, and service providers.

It turns out there is a simple solution to the impasses that dogged data breach legislation: incorporating data security provisions in federal privacy legislation without data breach notification.

The role of data security in the current privacy debate has been colored by this experience with data breach notification legislation. The conventional wisdom has been that data security is a poison pill—and when Senator Cantwell began to push to include data security in Senate Commerce legislation, there was concern that doing so could lead federal privacy legislation to the same fate as federal data breach notification legislation.

Data security appears in the solvable issues category of our privacy matrix because of this history and its importance as a privacy principle. But it turns out there is a simple solution to the impasses that dogged data breach legislation: incorporating data security provisions in federal privacy legislation without data breach notification.

Section 107 of COPRA and Section 204 of USCDPA provide for data security requirements but do not address data breach notification. They are almost identical in substance. Both call on covered entities to "establish, implement, and maintain reasonable … data security practices," tailor such practices to what is "appropriate to … the volume and nature of the covered data at issue," and enumerate some basic objectives for these practices. USCDPA adds that data security requirements should take into account "the size and complexity of the covered entity, the nature and the scope of the covered entity's collection or processing of sensitive data, [and] the volume and nature of the sensitive covered data at issue." COPRA uses more words to express substantially the same objectives.

COPRA frames data security as a Title I individual right; USCDPA makes it a Title II "data transparency, integrity, and security" provision. Given its origins in historical fair information practice principles, and its potential significance to individuals, we might be convinced to characterize data security as an individual right. But in operation, it is by nature more an obligation for covered entities. We could be persuaded by the flip of a coin.

The two Senate Commerce proposals do differ somewhat in how they provide for adaptations in data security requirements. USCDPA would grant the FTC rulemaking authority under the Administrative Procedure Act (APA) to adopt regulations, in consultation with the National Institute of Standards and Technology (NIST), "to identify processes for receiving and assessing information regarding vulnerabilities to sensitive covered data that are reported to covered entity." This authority could flirt with breach notification but could also operate as a way to collect information to assess national network vulnerabilities, which is within NIST's core

competence. Both bills also call for guidance from the FTC, but on different topics. USCDPA directs the FTC to issue guidance on identifying, assessing, and mitigating vulnerabilities of sensitive data, while COPRA directs the FTC and NIST to provide guidance on employee data security and privacy trainings.

As a general matter, we favor FTC guidance over rulemaking for cybersecurity and other rapidly evolving technical issues. This is especially true if the spectrum of entities and sectors covered under a federal privacy law were to increase. Guidance is more flexible and adaptable than formal rulemaking. We think a streamlined version of Section 204(c)(2) of USCDPA could include employee training—and, just as USCDPA already calls for NIST to contribute to rulemaking, it should play a role in guidance.

In the end, data security could be considered an implementation issue. The basic elements of data security are well-established and are mapped out by NIST, Securities and Exchange Commission sweeps, and boardroom briefings from security professionals—as well as legislation like GDPR, CCPA, and other state laws and regulations. As a result, the data security proposals in COPRA and USCDPA do not appear controversial and including data security provisions in comprehensive privacy legislation can help shore up national network security and data integrity.

We view the USCDPA and COPRA data security requirements as a template for similar provisions for baseline privacy obligations. They establish a few basic obligations framed with language about appropriateness in relation to scale and risk. We recommend using this approach more broadly as a regulatory model in privacy provisions and incorporating it into the proposed duties of loyalty and care as well as in privacy risk assessments.

Including data security provisions in comprehensive privacy legislation can help shore up national network security and data integrity.

C. Organizational Accountability

If Title I of a privacy bill describes individual rights *(See Part IV(A) of this report)*, then we recommend labeling Title II as "Responsibility and Oversight of Covered Entities." Under this proposed Title II, we recommend including an "Organizational Accountability" section, where we would combine some basic obligations for covered entities proposed in COPRA and USCDPA. We would also include under Title II separate sections for algorithmic decision-making *(See Part II(C) of this report)*, public privacy statements and disclosures *(See Part IV(C) of this report)*, data sharing *(See Part II(A) of this report)*, and data brokers *(See Part II(A) of this report)*. This proposed title would expand the content of Title II of COPRA, "Oversight and Responsibility," and combine much of Titles II and III of USCDPA, "Data Transparency, Integrity, and Security" and "Corporate Accountability."

Our proposed Title II structure seeks to highlight and reinforce two important elements of the bills. The first is the shift toward making the entities that collect personal data take the burden of protecting individuals' privacy interests. The second is to group together sections that focus on the processes by which these entities carry out this burden. As USCDPA's Title III heading recognizes, these processes have accountability in common.

These sections are an important complement to enforcement. Compliance does not happen automatically. Any legal or ethical compliance program—whether for financial integrity, health and safety, cybersecurity, or other recognized areas of corporate risk management and compliance—requires assessment, planning, responsibility, and ways of ensuring that plans and responsibilities are carried out. The same is true for privacy.

Compliance does not happen automatically. Any legal or ethical compliance program—whether for financial integrity, health and safety, cybersecurity, or other recognized areas of corporate risk management and compliance—requires assessment, planning, responsibility, and ways of ensuring that plans and responsibilities are carried out. The same is true for privacy.

In the first section within Title II, we would address the basic elements of organizational accountability. If nonprofits are included as covered entities, "organizational accountability" makes for a more inclusive heading than "corporate accountability."

RISK ASSESSMENTS

It is fitting that an organizational accountability provision would begin with privacy risk assessments, since any effective privacy program must start by assessing what data is collected, what processes and flows it undergoes throughout the data life cycle, and what privacy risks and other issues these present.[87] Both COPRA and USCDPA require risk assessments in some form.

Section 202 of COPRA requires covered entities to implement a "comprehensive written data privacy program and data security program," conduct annual "privacy and data security risk assessments, data hygiene, and other quality control practices," and otherwise implement compliance with the legislation. Section 107 of USCDPA explicitly requires large data holders to conduct "privacy impact assessments" within one year of the effective date and update assessments at least once every two years. COPRA couples privacy risk assessments with additional requirements—such as comprehensive privacy and security programs and appointment of privacy and security officers—that we suggest should be separate from a baseline privacy risk assessment requirement.

Because risk assessments are fundamental to privacy protection and the risk-based approach that informs a number of our recommended provisions, we believe it is necessary for them to be a requirement for all covered entities. Risk assessments would inform the requirement in our proposed duty of loyalty that a covered entity "establish reasonable policies and practices" to process and transfer data with respect for the privacy of individuals as well as the duty to avoid "reasonably foreseeable" harms under our proposed duty of care *(See Part II(A) of this report)*. It would help identify "potential risks to individuals" and "vulnerabilities" for purposes of establishing "reasonable data security practices" *(See Part III(B) of this report)*.

Thus, risk assessments belong in their own subsection, and we recommend moving the additional

requirements of COPRA (e.g., a comprehensive written data privacy program and data security program) to a different provision. After all, COPRA does not cover small businesses, and any additional requirements for covered entities to employ "qualified" privacy officers and prepare annual or biannual comprehensive written assessments could amount to an unnecessary burden for many SMEs where the scale and risk of privacy harms might not warrant it. On the other hand, we see no reason why privacy risk assessments should be limited to large data holders, especially as Section 107 of USCDPA provides that such assessments be "reasonable and appropriate in scope" based on scale, complexity, and risk. This modifier mirrors the USCDPA data security provision (Section 204), which applies to all covered entities but is scaled according to size and scope. A privacy risk assessment tailored in this way would be no more onerous than scaled data security requirements applicable to all covered entities.

Indeed, we believe the tailoring factors listed in USCDPA Section 107 (a)(2) –

- *the nature of the covered data collected, processed, or transferred by the covered entity;*
- *the volume of the covered data collected, processed, or transferred by the covered entity;*
- *the potential risks to the individuals from the collection, processing, or transfer of covered data by the covered entity; and*
- *the size and complexity of the covered entity.*

should shape the frequency as well as scope of privacy risk assessments. To the second factor, we recommend adding "the volume and uses of the covered data" since use can have a material impact on risk. As in USCDPA, the language should spell out that the assessment should weigh the benefits of collection, processing, or transfer against "the potential adverse consequences to individual privacy."

> Because risk assessments are fundamental to privacy protection and the risk-based approach that informs a number of our recommended provisions, we believe it is necessary for them to be a requirement for all covered entities.

In turn, Section 107(b) of USCDPA details requirements for large data holders to conduct written privacy impact assessments, which is another graduated layer of accountability. To this provision, we suggest adding an obligation to make the written assessment available to the FTC upon request—mirroring the algorithmic decision-making impact assessment section—because we recommend treating algorithmic decision-making impact assessments for large data holders as an add-on to the detailed written privacy and security risk assessments for all covered entities.

As with other recommendations in this report, this tailored approach to risk assessment would establish a significant safeguard for individual privacy while avoiding a one-size-fits-all prescription. It preserves flexibility for a wide variety of entities and use cases, but would undoubtedly be informed by best practices, experience, and risk management. In turn, we would maintain a graduated approach to regulation by applying additional obligations to

large data holders—such as to maintain privacy risk assessments in written form for at least five years and submit them to the FTC upon request.

ADDITIONAL ACCOUNTABILITY

We suggest that the COPRA and USCDPA requirements for appointment of privacy and security officers and development of comprehensive written privacy and security programs also belong under the heading of "Organizational Accountability," but in a separate provision that applies to all covered entities above the ceiling for SMEs. We do not think this provision needs to specify an annual requirement, because it would be subject to the underlying obligation to conduct a risk assessment "appropriate in scope and frequency" in light of the factors listed above.

There is one additional layer of accountability that we recommend adding for large data holders. Section 201 of COPRA ("Executive Responsibility") requires the CEO of any large data holder, along with the chief privacy officer and chief security officer, to annually certify to the FTC that the covered entity maintains "adequate internal controls" and reporting structures for compliance, based on an internal review. We suggest incorporating this provision into the section on corporate disclosures we discuss later *(See Part IV of this report)*.

As with similar executive certification requirements under the Sarbanes-Oxley Act, such a requirement raises the stakes for management of public companies.[88] With this in mind, we recommend raising the threshold for "large data holders" in COPRA and USCDPA, where the definition applies to covered entities that process covered data from more than 5 million individuals or sensitive covered data from more than 100,000 individuals. We think these levels are over-inclusive—the sensitive data threshold, for example, could sweep in many relatively smaller health care providers and insurers. Instead, we suggest more targeted levels of 30 million (approximately ten percent of the U.S. population) and three million, respectively.

We include this provision based on the example of elevating cybersecurity as a C-suite issue. Along with repeated jawboning on the need for boardroom attention to cybersecurity, the Securities and Exchange Commission forced upper-management level attention by requiring disclosure of information risk and making cybersecurity management a subject for broker-dealer sweeps.[89] Executive certification could have a similar effect for privacy. The management changes that privacy issues forced at Uber and the recent experiences at Zoom are a cautionary tale about the impact that poor attention to privacy risks can have on trust in the marketplace.[90] No CEO can afford to say, as Zoom CEO Eric Yuan recently had to, "I really messed up" on privacy and security.[91]

D. Federal and State Enforcement

The foundational elements of federal and state enforcement in USCDPA and COPRA bear many similarities, but with a few important differences. In drawing some key points from both bills, we suggest an approach that provides strong tools for federal privacy enforcement along with a robust role for states to play. COPRA treats federal, state, and individual enforcement together in one lengthy section, while USCDPA breaks them out into separate sections. We found the latter approach easier to parse.

We previously discussed the private right of action in Section I(B)—and in this section, we discuss our recommendations on federal and state enforcement.

EMPOWERING THE FTC

A threshold question in any proposed U.S. privacy legislation is what agency should enforce it. The prevailing view among current bills and stakeholder proposals is that the Federal Trade Commission should continue in its role as America's principal privacy enforcement authority but be given increased legal authority and resources. This is the approach COPRA and USCDPA take.

Some members of Congress, academics, and privacy advocates[92] have supported the creation of a new agency, modeled after the Consumer Financial Protection Bureau and the European concept of a "data protection agency" ("DPA"). Representatives Eshoo and Lofgren's Online Privacy Act of 2019 included the creation of a DPA. More recently, Senator Kirsten Gillibrand (D-NY) introduced her Data Protection Act of 2020 to create a DPA.[93]

We agree that the FTC is the right answer to this important question. As Chris Hoofnagle, Woodrow Hartzog, and Daniel Solove—all leading scholars on the FTC's role in privacy—argue, "the FTC is still the right agency to lead the US privacy regulatory effort…. But it does need to evolve to meet the challenge of regulating modern information platforms."[94] Even with limited resources and constrained legal authorities, the FTC has become one of the leading privacy enforcers in the world, and it has a strong reputation and relationship with its peer data protection agencies across the globe. Its record for bipartisan collaboration stands out among independent agencies in the federal government, and it has an experienced professional staff. Whatever limitations it has, there is no guarantee a new agency would do better—and it in the meantime, a new agency would have to ramp up without the existing resources and experience the FTC has.

We also agree with Hoofnagle, Hartzog, and Solove that for the FTC to meet the privacy challenge, Congress must give the Commission "more resources, more tools, a greater shield from political pressure, and a clear Congressional mandate." In a series of public appearances at Brookings, FTC commissioners from both parties have emphatically said that the agency cannot carry a statutory privacy enforcement mandate without these.[95] The elements of agreement between USCDPA and COPRA provide a good start for empowering the FTC, especially when coupled with some proposals that are included in only one or the other of those bills.

Even with limited resources and constrained legal authorities, the FTC has become one of the leading privacy enforcers in the world.

FTC reach, capabilities, and tools

The basic outline of FTC enforcement is straightforward in both USCDPA and COPRA. Both propose to treat violations of the legislation as violations of the FTC's unfair and deceptive practice authority and of regulations pursuant to this authority, with basic powers guided by the FTC Act.[96] Both bills also share the concept of a "data privacy and security relief fund" to both help compensate victims of privacy violations and provide additional tools to the FTC. In addition, both include placeholder authorizations for appropriations to carry out the legislation.

By deeming a violation of privacy legislation to be a violation of regulations under the FTC Act's unfair and deceptive practice provision, both bills address an essential need: giving the FTC the authority to seek penalties for initial privacy violations. Under current law, the FTC is able to seek penalties only for violations of existing consent orders or regulations. For example, the FTC could not seek civil penalties when issuing an initial consent order against Facebook in 2012—but its settlement with Facebook in 2019 included a $5 billion penalty, following the Cambridge Analytica investigation.[97] COPRA and USCDPA reflect the broad support for enlarging this authority.

Nonprofit organizations—some of which are far larger than most U.S. for-profit companies—can manage significant amounts of data and have significant impacts on Americans' privacy.

Their approach would bring to bear Section 5(m) of the FTC Act, which applies to "knowing violations" of rules.[98] It requires "actual knowledge or knowledge fairly implied on the basis of objective circumstances" that an act is prohibited. This means that not every violation of a baseline privacy law would be subject to FTC penalties. But we think this authority would reach serious violations. As interpretation of the law becomes more established through regulations, guidance, cases, codes of conduct, and best practices, the force of the "implied" knowledge provision would ratchet upward. And the knowledge standard under Section 5(m) parallels our recommended approach to the private right of action in filtering overly technical "gotcha" cases.

With regard to enhancing the scope of FTC authority and resources, there are four valuable proposals that flow from USCDPA, COPRA, and other sources. First, as discussed above in connection with covered entities *(See Section III(A) of this report)*, USCDPA includes common carriers and nonprofits within the reach of the FTC privacy enforcement. By including common carriers, legislation would ensure that the majority of Americans' online engagement would be covered by the same set of rules and regulations, thereby reducing confusion for individuals and ensuring a level competitive playing field for covered entities. And nonprofit organizations—some of which are far larger than many U.S. for-profit companies—can manage large amounts of data and have significant impacts on Americans' privacy.[99]

Second, COPRA proposes a new bureau to focus on privacy enforcement within the FTC; we recommend taking it a step further by specifying a minimum number of professional staff—including attorneys, technologists, and economists—to ensure that the Commission has the internal capacity to vigorously enforce national privacy standards. While our suggestion that the FTC hire at least 500 professional staff for a new privacy bureau may seem large to some, it would make the bureau comparable in size to the United Kingdom's Information Commissioner's Office, responsible for privacy in a country about one-fifth the size of the United States.[100] Senator Moran's CDPSA proposes a staff of 440, and based on the UK ICO comparison, Microsoft senior vice president and former FTC commissioner Julie Brill endorsed 500 in response to a Senate Commerce hearing question from Chairman Wicker.[101]

Third, in addition to bringing to bear civil penalty authority, we believe that privacy legislation should offer guidance on how the FTC should set civil penalties. Drawing on CDPSA, we suggest maintaining the current civil penalty limit at $43,280 per violation, adjusted annually for inflation,[102] but giving statutory guidance to the FTC and courts on the amounts of fines and factors to be considered. This will ensure that the gravity of the violation and the size and sophistication of a covered entity are taken into account in any civil penalty.

Finally, we agree with COPRA that the FTC should have independent litigation authority. This authority would allow the agency to initiate civil actions in privacy and security cases on its own, without relying on the Department of Justice (although the FTC would still be able to seek engagement by Justice). This independence is appropriate for the lead U.S. privacy enforcement authority and would allow the Commission the flexibility to pursue cases of its choosing even if the Department of Justice is overburdened or has other enforcement priorities. Such authority undoubtedly would meet opposition from Justice. But that department does not have deep expertise in commercial privacy and should not act as a filter for enforcement decisions that reflect judgments about privacy policy, technological developments, and coordination with international privacy enforcement partners that are within the FTC's expertise.

FTC rulemaking authority

Substantive rulemaking authority for the FTC has been a challenging issue for more than 30 years. While the Commission has rulemaking authority for procedural implementations of new federal laws, the Magnuson-Moss Act reflected a congressional desire to curb the FTC's substantive rulemaking by limiting its ability to issue rules under the Administrative Procedure Act.[103] In the privacy arena, as we (Kerry, with Daniel Weitzner) have written,[104] we would have concerns about a privacy bill that leaves it up to the Commission broadly to set the basic rules to address privacy (as some bills propose).

> Privacy rules require some hard choices, and Congress is best situated to make those choices.

We believe that the substantive rights and obligations at the heart of any privacy law should be determined by Congress, and not be left to a grant of broad rulemaking authority.[105] Privacy rules require some hard choices, and Congress is best situated to make those choices—ideally by articulating some broad rules and principles that provide meaningful privacy protection without imposing unduly prescriptive and inflexible rules. We recognize that there are also "more technical areas where rulemaking can help fill in details and keep up with changes in technology and the marketplace."[106] USCDPA and COPRA adopt such an approach by delegating specific rulemaking authority to address particular issues to the FTC, for example to identify additional categories of "sensitive data" that may arise over time.

We support this delegation to address implementation questions or keep up with evolving technology. We also propose some additional areas for focused rulemakings that are not advanced in either USCDPA or COPRA. For example, the process of defining which nonprofit entities should be treated as "small or medium entities" would benefit from input through a rulemaking procedure. We also recommend that

the Commission be able to conduct a rulemaking to identify other types of data or situations that warrant additional exceptions to the requirement of "affirmative express consent," in order to address situations where the added burden on individuals proves to significantly outweigh the value of the consent. Similarly, to avoid confusion as technology evolves, we suggest giving the FTC authority to clarify whether particular pieces of equipment fall into the definition of "device."

For reasons elaborated in the Kerry and Weitzner article, we do not support the broad and general rulemaking authority that COPRA would grant to the FTC in Section 110(h), which authorizes APA rulemaking for any of the provisions in Title I of the bill. COPRA's Title I incorporates a robust and fairly comprehensive set of privacy rights and obligations that we generally support and propose strengthening in various respects. Some of these rights and obligations warrant specifically-articulated rulemaking authority. But we do not believe that there should open-ended additional authority to impose regulations.

Strong congressional action to enhance the Commission's powers and authorities would allow it to build on this track record.

Issue-specific certification programs

USCDPA (Section 403) proposes the possibility of "certification programs" to allow associations, other groups, or individual covered entities to develop—with FTC review and approval—concrete guidance on how to satisfy their obligations under legislation. This type of program can be beneficial because it can provide particular sectors with specific guidance on how to comply with federal privacy law, tailored to sector-specific issues in ways that can be more granular than most agency regulations. Similarly, they can provide more on-the-ground compliance oversight than an agency is likely to provide. In our view, one value of this kind of compliance program is that most companies do not operate out of ill motive, but rather lack privacy policy knowledge and seek certainty to manage their risks. In this light, many such companies—as well as individuals—could benefit from guidance about how best to comply with privacy rules and regulations that is tailored to specific sectors, issues, or applications.

To ensure such programs do not operate as a blank check for self-regulation, there needs to be strong oversight to ensure guidance actually does protect privacy consistently with the federal law and establish meaningful compliance mechanisms. The goal and focus of such programs must not be on self-certifications that an entity complies with the legislation, but on mechanisms that ensure full compliance by covered entities that adopt and follow a program. To these ends, we recommend changes to reinforce the mechanism advanced in USCDPA.

When reviewing proposed programs, we suggest the FTC consider whether the program was developed in consultation with academic, civil society, and other privacy and security experts. We also recommend that any compliance program be time-limited, with industry sectors required to return to the FTC after an initial interval of four years to seek renewal and approval to continue using a certification program. This would ensure that the practices in the program keep pace with changes in technology, industry conditions, and privacy practices, and that programs that are not effective must change or be discontinued.

One additional important change we suggest is that (other than a rulemaking on procedures for certification programs) the entire system not go into effect until two years after the effective date of the federal privacy law. This delay would allow the FTC to complete a range of substantive rulemakings that would set some of the more granular regulations, allowing covered entities to become familiar with the rules before proposing compliance programs. The delay also would allow the Commission to manage its staffing resources to focus first on required regulations before turning to compliance programs. Finally, the delay would allow everyone—covered entities, privacy advocates, and the FTC—to gain some experience with the newly passed legislation before filling in gaps with proposed compliance programs.

Together, the various authorities and capabilities suggested above would provide the FTC with a strong ability to enforce federal privacy legislation robustly and effectively. The Commission already has an effective track record as a privacy enforcer, but with limited capacity and without a strong law to enforce. Strong congressional action to enhance the Commission's powers and authorities would allow it to build on this track record.

STATE ENFORCEMENT

In addition to strengthening FTC authority and resources—and consistent with both USCDPA and COPRA—a federal privacy law should allow state attorneys general to enforce the federal standards. COPRA and USCDPA both reflect the broad spectrum of support for a state role in enforcing a federal privacy law, including among industry. From a privacy enforcement perspective, state attorney general offices offer tremendous reinforcement to the capacity of the FTC, and local officials would be better positioned to address local concerns and smaller privacy violators. And as noted in Part I(A) of this report, state attorney general enforcement is an essential corollary of any proposal to preempt state laws. It would be simply be untenable to preclude all state involvement in the protection of privacy and data security, which are issues of concern everywhere.

Both COPRA (Section 301(b)) and USCDPA (Section 402) specify state attorneys general, or any consumer protection officers authorized by states, to bring such cases. As a matter of federalism, the federal government should not specify which state officials can bring civil actions—and so COPRA and USCDPA take the right approach in enabling state-authorized privacy or consumer protection officials to act, should states make such a choice.

At the same time, the FTC should be able to remain the guiding force for the overall development and enforcement of the federal law. USCDPA and COPRA both recognize the importance of federal supremacy in the administration of a privacy law by requiring that actions by state attorneys general be brought in federal court, and by authorizing the FTC to intervene as a matter of right and be heard on all matters in any action brought by a state official. We suggest going one step further than intervention to allow the FTC to step in and assume responsibility for prosecuting an action initially brought by a state official. We expect that this ability would be exercised by the Commission rarely, but it would make it possible for the FTC to ensure that state cases do not interfere with the national privacy regime—for example, by pushing too narrow or too broad a reading of federal law.

This combined federal-state approach to enforcement will be robust enough—and ground-level enough—to strengthen the data privacy and security of all Americans under the federal privacy umbrella.

IMPACT ON OTHER FEDERAL LAWS

USCDPA and COPRA both generally leave undisturbed the existing "silos" of U.S. sectoral privacy laws—such as those applicable to medical records and credit reports—and both include language that avoids disrupting those laws. We agree with this approach as a necessary expedient to filling the growing gaps in current law but recommend that a comprehensive federal privacy law be even more specific about how the new legislation would interact with existing law.

To this end, we suggest federal privacy legislation include a thorough list of existing privacy laws and a clear statement that—to the extent that certain information is covered both by the legislation and by an existing statute—a covered entity in compliance with these existing laws would be deemed in compliance with the legislation. The table below sets out this list from our research.

Table 5: Federal Laws Savings Clause
We recommend that federal privacy legislation state that "a covered entity that is required to comply with one of the following federal laws, and is in compliance with data privacy requirements of that statute, shall be deemed in compliance with federal privacy legislation."*

1. Title V of the Financial Services Modernization Act of 1999 (15 U.S.C. § 6801 et seq.).
2. The Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17931 et seq.).
3. Part C of title XI of the Social Security Act (42 U.S.C. § 1320d et seq.).
4. The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.).
5. Section 444 of the General Education Provisions Act (20 U.S.C. § 1232g) (commonly referred to as the "Family Educational Rights and Privacy Act").
6. Regulations promulgated pursuant to Section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d–2 note).
7. The Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.).
8. The Fair Debt Collection Practices Act (15 U.S.C. § 692 et seq.).
9. The Controlling Assault and Non-Solicited Pornography and Marketing Act (15 U.S.C. § Chapter 103).
10. The Restore Online Shoppers' Confidence Act (15 U.S.C. § 8403).
11. The Telemarketing and Consumer Fraud and Abuse Prevention Act (15 U.S.C. § 6101 et seq.).
12. The Telephone Consumer Protection Act (47 U.S.C. § 227).
13. The Genetic Information Nondiscrimination Act (42 U.S.C. § 2000ff).
14. Section 222 of the Communications Act of 1934, as amended, insofar as it relates to use of information necessary to provide emergency services or to address anticompetitive behavior based on customer usage of existing services (47 U.S.C. § 222).
15. The Electronic Communications Privacy Act (18 U.S.C. § 2510 et seq.).
16. The Driver's Privacy Protection Act (18 U.S.C. § 2721 et seq.).
17. The Federal Aviation Act of 1958 (49 U.S.C. § 1301 et seq.).

*For (4), (5), and (7) through (17), we recommend that proposed data security requirements continue to apply to such entities.

This list is consistent with some elements of COPRA but supplements it with additional statutes. We also recommend that within one year of enactment of legislation, the FTC—in consultation with relevant agencies—should issue guidance on any overlaps of the differing federal privacy regimes in consultation with the applicable agencies.

Looking to the future, we recommend that Congress establish a "Commission on Harmonization of Federal Privacy Laws" effective five years after the legislation becomes law. This proposed commission would be charged with evaluating the effectiveness of existing federal privacy regimes and making recommendations about how federal laws addressing privacy and data security might be harmonized. Over the long term, it would be less confusing for individuals and businesses both if the privacy rules that apply to one industry were similar to (if not the same as) the privacy rules that apply to another industry. From an individual's vantage point, the activities of credit agencies and data brokers or the functions of fitness bands and medical devices might look similar, but differing privacy regimes will apply in these cases. From the standpoint of a business that offers overlapping products or services, a single regime would be simpler.

Developing a new privacy law applicable to all entities throughout the country—to replace existing privacy laws applicable to some major industry sectors—would be an enormous undertaking. For the time being, and at a minimum, it would be appropriate for a commission to analyze the situation and make recommendations to Congress.

Part IV – The Implementation Issues

KEY RECOMMENDATIONS

- We recommend combining the individual rights to request access, correction, deletion, or portability of personal information into an overarching "Right to Control" section and adding a separate "Right to Recourse." Small or medium entities should be exempt from these two provisions.

- Effective transparency mechanisms cannot be one-size-fits-all. Covered entities should be required to provide three layers of transparency: a) timely, context-specific notifications for individuals, b) basic disclosures targeted to individuals, and c) comprehensive privacy disclosures targeted to regulators and other specialized parties. While all covered entities should be required to comply with each of these three formats, large data holders should face additional obligations (e.g., to annually certify their comprehensive disclosure statements to the FTC).

- A bill title should reflect that individuals have a privacy interest in all types of information, and not merely "data," online information, or consumer transactions. We thus recommend the "Information Privacy Act."

- Privacy legislation should take effect immediately upon enactment to allow time for necessary FTC rulemaking, but certain provisions (e.g., the right to control and right to recourse) should have tiered effective dates to allow covered entities time to become compliant with certain provisions. Governmental enforcement should be delayed until six months after the effective date of the applicable FTC regulations, as with CCPA, and private actions should not be permitted until two years after the effective date of the law.

A. Right to Control

Individual rights to access, correct, delete, and request portability of personal information have been a central element of most recent privacy proposals.[107] These include not only COPRA, USCDPA, CDPSA, and the House Energy and Commerce draft, but also some of the most business-oriented proposals like those of the U.S. Chamber of Commerce and the Internet Association.[108] This bipartisan support and widespread agreement especially reflect the impact of GDPR and CCPA, which have set worldwide expectations for individual privacy rights and caused many U.S. businesses to implement such rights.

Such individual rights to information in the custody and control of covered entities recognize an essential element of privacy: that individuals retain interests in the personal information they share with others and that—rather than exercise absolute dominion over this information—the organizations that receive it exercise shared control over the information. As we (Kerry, Chin) have written, rights like these "offer a path to greater individual agency over online personal information, no matter which service or product people use."[109] While we believe the single most important function of baseline privacy legislation must be to set norms for the collection, processing, and transfer of personal information, such individual agency can act as an important check and a means to fine-tune broad norms to individual expectations.

While the majority of individuals probably will not exercise these rights, to some people they will matter a great deal. For example, when Microsoft implemented GDPR data subject rights for customers outside the European Union, it found that about 6.7 million U.S. residents used its "privacy dashboard" in the first year of implementation, compared to 4 million EU residents.[110]

COPRA and USCDPA share substantially identical provisions to provide individuals with these four rights upon receiving verified requests. Both proposals require covered entities to provide individuals with access to personal data—or an "accurate representation" of this information—as well as with the names of third parties to which covered data has been transferred and the purpose of transfer. Both enable individuals to ask covered entities to delete covered data, correct inaccuracies or incomplete information, and receive covered data (with the exception of derived or inferred data) in a portable, interoperable, and unlicensed format.[111] And both require covered entities to inform service providers or third parties to do so as well.

Individual rights to access, correct, delete, and request portability of personal information have been a central element of most recent privacy proposals.

There are a few differences in details between the two proposals. COPRA details each of these rights individually in separate sections (Sections 102, 103, 104, and 105), while USCDPA groups all four together under a "right to control" (Section 103). USCDPA provides access to the names of both service providers and third parties that have received covered data, while COPRA requires access only to the names of third parties. USCDPA allows covered entities either to de-identify or to delete data upon request, while COPRA only allows them to delete the data. USCDPA requires covered entities to address verified requests

in no more than 45 days—and fulfill them at no cost at least twice in a 12-month period—while COPRA does not specify a time period and mandates that all requests are free of charge.

With respect to each of these differences, we believe USCDPA takes the better approach for varying reasons. Grouping all four of these rights under the umbrella of a "right to control" avoids repetition and simplifies exemptions, making them easier to understand and implement. Setting a 45-day deadline for covered entities to address verified requests is common sense to ensure accountability and avoid delay. Similarly, providing these four rights free of charge empowers individuals, while capping requests to twice within any 12-month period prevents the costs to covered entities from multiplying.

Requiring entities to provide the names of service providers—in addition to third parties—to which data has been transferred would provide additional transparency. This information would allow insight into the care with which a covered entity handles data, as well as the extent of information-sharing ecosystems. It is startling to see, for example, the number of entities that receive HIPAA-protected information as "business associates," the HIPAA analogue to "service providers."[112]

Giving covered entities the choice to either delete or de-identify covered data upon receiving a verified request recognizes the shared interests that both individuals and covered entities have in the information. This provision would allow covered entities to derive beneficial use of such information, subject to requirements in the definition of "de-identified data" in both proposals to prevent the residual risk of re-identification.

In addition to these recommendations, we propose one modification to the way USCDPA frames these individual rights. Although both USCDPA and COPRA require covered entities to provide access to covered data, COPRA (Section 2 (8)) includes "derived data" in its definition of "covered data" and USCDPA (Section 2 (7)) does not. Therefore, we recommend clarifying that covered entities must also provide individuals with access to any derived data linked to them. This would provide transparency functionally equivalent to icons and buttons that link to reasons why a person has received an advertisement; these provide a small glimpse of what picture platforms or advertisers have of the recipient. This, in turn, helps provide some understanding about data collection and how one's online behavior can be interpreted.

An overlooked issue concerning the right of access arises from the gig economy, where large companies may indirectly partner with non-employee contractors (or gig workers) to deliver a service. We call this the "DoorDash problem," based on a specific use case that arose in discussion: if a restaurant company contracts DoorDash to deliver takeout food, and DoorDash subsequently subcontracts with someone to conduct deliveries, is that person considered a "third party" or "service provider" under these provisions? If so, and somebody requests a full list of entities that have received personal information, must the restaurant company be able to name each DoorDash contractor upon individual request or in public disclosures? To address these questions, we suggest adding a clarification to the public disclosure provision that covered entities should be required to identify the contracting service provider (DoorDash) but not the end service provider (individual gig workers) in these cases. We also suggest a modification to the definition of "service provider" in both COPRA and USCDPA.

As discussed in connection with exceptions for small and medium entities, we recommend that small or medium entities should be exempt from the requirements of the "right to control," as well as the "right to recourse" in the following section.

B. Right to Recourse

We propose the addition of another individual right: a "right to recourse." This addition would provide a mechanism for individuals to seek remedies not covered by data access, correction, deletion, and portability. In addition, individuals might want to escalate an organization's denial of one of these four requests, and covered entities may value the opportunity to address privacy disputes without litigation.

This right to recourse is patterned on provisions in the EU-U.S. Privacy Shield framework that enables transfers of data about EU residents from the European Union to the United States. Companies that certify under the Privacy Shield are required to provide "recourse mechanisms" enabling individuals to raise complaints and receive a response within 45 days.[113] Recourse mechanisms were adopted to provide rights equivalent to those under European data protection law—now reflected in the GDPR. The 2019 Washington Privacy Act also included a right to recourse, and we use it as a model for our proposed provision.[114]

In this provision, covered entities would need to establish an internal process by which individuals may seek recourse for privacy complaints not otherwise addressed by the "right to control." Individuals could also use the "right to recourse" to appeal the refusal to act upon a request of data access, deletion, correction, or portability. This internal complaint process should be conspicuously available and easy to use, and covered entities should inform individuals of any related action taken within 45 days. In responding to the right to recourse, we recommend that covered entities also be allowed to make offers of monetary compensation to individuals. All covered entities should be responsible for compliance with this right, except for small or medium entities.

We propose the addition of another individual right: a "right to recourse." This addition would provide a mechanism for individuals to seek remedies not covered by data access, correction, deletion, and portability.

In our discussion of the scope of a private right of action *(See Part I(B) of this report)*, we discuss how this recourse provision can be used to provide notice and an opportunity to cure prior to litigation and provide an opportunity for a litigation cost-shifting mechanism like that under Rule 68 of the Federal Rules of Civil Procedure.

In our discussions with stakeholders, this idea was well-received. It offers a form of consumer remedy—and by signing up for the Privacy Shield, more than 5,000 U.S. companies have already agreed to provide a similar right.[115] Implementing an explicit right to recourse in U.S. federal privacy law could offer some help in likely future EU-U.S. data transfer negotiations since recourse is an important element in the European Commission's review of U.S. privacy protection. Thus, the inclusion of a "right to recourse" in U.S. federal privacy legislation should not be controversial.

C. Notice and Transparency

Transparency has been a keystone of information privacy regulation since the development of fair information practice principles.[116] It has been integrated into the practices of U.S. companies through the widespread adoption of privacy notices and embedded in laws like the Gramm-Leach-Bliley Act of 1999[117] and, more recently, CCPA and GDPR.

Notice and transparency are not sufficient on their own, but they are a necessary element of privacy regulation.

Currently, notice and transparency carry too much of the load of protecting individual privacy and put too much of this load on the individuals themselves. For the average person who encounters dozens of websites, apps, and other services on a daily basis, reading a barrage of privacy policies is unrealistic and even useless. Even before the widespread adoption of smartphones, Aleecia McDonald and Lorrie Faith Cranor estimated in 2008 that it would take the average U.S. internet user 76 work days to read privacy policies from every website they visit.[118] As we (Kerry) have written, "at the end of the day, it is simply too much to read through even the plainest English privacy notice."[119]

Notice and transparency are not sufficient on their own, but they are a necessary element of privacy regulation. Individuals should have access to information about data and their rights—and some demand this access. When affirmative express consent is required to provide a service, individuals need relevant information prior to consenting. Moreover, privacy policies can be important to other audiences—for example, the Federal Trade Commission uses them as benchmarks for deceptive privacy practices and has brought cases against companies that violate their own privacy policies.[120] As we elaborate below, we believe privacy legislation needs to incorporate notice and transparency in ways that recognize these different functions.

NOTICE AND TRANSPARENCY IN COPRA AND USCDPA

Most current bills or draft bills include notice and transparency provisions, and COPRA and USCDPA are no exception. Section 102(b) of COPRA articulates a "right to transparency." It requires covered entities to publish in a prominent and accessible way "a privacy policy" that provides a "detailed and accurate representation of the entity's data processing and data transfer activities." The information must include the identity and contact information of the covered entity, categories of data collected, purposes of processing, categories of service providers and third parties to which data is transferred, identities of third parties that data is transferred to, and purposes of transfer. Covered entities also are required to publish the length of data retention, how individuals can exercise their individual rights under the legislation, a description of the covered entity's data security policies, and the effective date of the privacy policy. COPRA also groups the rights to access and transparency together in Section 102.

The corresponding Section 102 of USCDPA, which is entitled "Transparency," also requires covered entities to publish "a privacy policy" that must be publicly available "in a clear and conspicuous manner" and

disclosed to individuals prior to or at the point of data collection. The required content of the policies is similar to COPRA—with some minor differences—but it differs from COPRA in requiring disclosure of privacy policies for every event of data collection.

COPRA and USCDPA both have additional provisions requiring covered entities to notify individuals for affirmative express consent requests and for material changes to privacy policies. The COPRA consent notification provision is part of its definition of affirmative express consent (Section 2(1)). It requires a "standalone disclosure" as part of a request for consent in "easy-to-understand language." The disclosure must describe "each act or practice" with "prominent headings" and in terms that distinguish what is necessary for something requested by the individual from other purposes. The transparency provision requires affirmative express consent for a material change in a privacy policy or practices for covered data "that would weaken the privacy protections applicable," and also "direct notification, where possible" to affected individuals.

USCDPA's counterpart is part of its consent section (Section 104) and contains similar requirements: "a notice" that must describe the "processing purpose," distinguish between a purpose necessary to fulfill a request and other purposes, have a "prominent heading" associated with the purpose, and "explain the individual's right to provide or withhold consent." In turn, USCDPA applies the requirements for affirmative express consent to "a material change in [a covered entity's] privacy policy."

DISTINGUISHING FUNCTIONS OF NOTICE AND TRANSPARENCY

By differentiating between requirements for individual notifications in the context of consent and those for published privacy policies, COPRA and USCDPA appear to recognize the absurdity of using privacy policies or terms and conditions as a basis for consent and the differing functions of notifications and privacy policies. We believe, however, that to make notice and transparency more effective, the bills need to go farther in differentiating functions and tailoring content requirements accordingly.

We (Kerry, Chin) have written that descriptions of privacy policies and practices have different uses for different contexts and audiences. We categorize these here as follows:

- timely, context-specific notifications for individuals ("notifications");
- basic descriptions aimed at a general audience of individuals ("privacy statements"); and
- comprehensive privacy disclosures targeted to regulators and other specialized parties ("comprehensive disclosures").

We recommend that, to make notice and transparency more effective for individuals and for accountability, privacy legislation should reflect these different audiences and functions with distinct requirements for notifications and privacy statements, and a separate provision for comprehensive disclosures.

Timely, context-specific notifications for individuals

Individuals benefit from targeted, relevant information in multiple formats and contexts, and we seek to reinforce that one-size-fits-all disclosures do not work for most people. COPRA and USCDPA recognize this in significant ways by requiring requests for affirmative express consent to provide a description of the relevant processing act, the choice to consent or refuse, and ways to exercise privacy rights.

We suggest an individual right to transparency section include more general application of similar requirements for any kind of individual notification and enumerate more broadly circumstances in which notification is mandatory. In general, we think covered entities should provide individuals with simplified, timely, and actionable notifications in specific contexts, such as: (a) when affirmative express consent is required for the collection, processing, or sharing of sensitive covered data, (b) in the event of certain changes in privacy policies, and (c) should the government request, subpoena, or warrant covered data relating to an individual.

Keeping this list narrow would help provide people with basic and relevant information while also mitigating the "consent fatigue" that comes with constant privacy notifications.[121] Such privacy notifications should vary by context and situation, but we would conceptually reflect the COPRA and USCDPA affirmative express consent provisions by requiring that they "present clear, fair, and concrete choices of actions to take in response," specifically identify what data is involved, the purpose of processing, and "why the data is needed for such purpose," and clearly explain how to consent or opt out.

Basic privacy statements

Contextual notifications may be all the interaction many people have with information about covered entities' data privacy policies and practices, but they are not enough. Additional information should be available for anybody who wants to know more, and in order for the five individual rights to be effective, people need to know what these rights are and how to exercise them.

We propose the term "privacy statements" for two reasons. One is to differentiate them from the status quo today; the second and more important one is because U.S. internet users might erroneously believe that a "privacy policy" means that companies keep all collected information private—as a 2014 Pew Research Center survey would suggest.[122]

As specified in COPRA and USCDPA, we recommend that these privacy statements include the categories of data used, categories of third parties that data is shared with, purposes of use, length of data retention, and the ways individuals can exercise their privacy rights. We recommend saving some of the more technical COPRA and USCDPA transparency provisions for the comprehensive privacy disclosures, such as the categories of service providers to which data is transferred, identities of third parties which data is transferred to, description of data security practices, and effective date of the privacy policy, but we recommend including links to additional information where applicable.

COPRA also requires covered entities to publish a "detailed and accurate representation of the entity's data processing and data transfer activities." For the purposes of providing simplified privacy statements, we recommend removing the "detailed" provision and requiring basic privacy statements to include descriptions of data collection, processing,

and sharing practices for each product or service that it provides.

We recommend a clause communicating that the public statements or descriptions of privacy policies and practices are distinct from the comprehensive disclosure statement described below, but may link to each other or overlap some content. This would make clear for covered entities designing these privacy statements that the statements are not meant to replicate the long and complex legal documents that many privacy policies resemble today.

Comprehensive privacy disclosures

Finally, we recommend adding a section to the obligations of covered entities that requires covered entities to make more comprehensive public disclosures available about their data processing, privacy, and security policies. Here, we emphasize the word "comprehensive:" we propose that these disclosures provide a "detailed, complete, and accurate description" of the data processing, transfers, and policies and practices.

These disclosures would include information parallel to that in the basic privacy statements, plus the methods of data collection, the processing purpose for collection, a summary of how data is used for algorithmic decision-making, the category and identity of each third party to which data is transferred, a description of the covered entity's data security practices, identification of reported data breaches for the past three years, and how individuals or organizations can request to receive notifications of changes in privacy policies. We see these comprehensive disclosures as complementary to risk assessments and other accountability measures in necessitating attention to what covered data is collected, how it is processed and shared, and how these affect individual privacy and compliance with privacy law. In the case of large data holders, these disclosures would be reinforced by executive certifications as discussed above.

> Not all data collection occurs on the internet and individuals have privacy interests that extend beyond their interactions with companies as consumers.

Since these disclosures would be conspicuously available to the public, any interested person would be able to read them. But the primary audience is regulators, watchdogs such as journalists and privacy organizations, and researchers. Requiring that the disclosure be in machine-readable format would enable comparison across covered entities.

D. Title

Many of the privacy bills or draft proposals over the past two years use the words "consumer," "online," and "data" in their titles. These include Senator Cantwell's Consumer Online Privacy Rights Act, Senator Wicker's United States Consumer Data Privacy Act, Senator Moran's Consumer Data Privacy and Security Act, Representatives Eshoo and Lofgren's Online Privacy Act, among others.[123]

Certainly, a vast amount of data collection and processing occurs online and in the context of consumer-business relationships. However, not all data collection occurs on the internet and individuals

have privacy interests that extend beyond their interactions with companies as consumers. Referring to privacy as a "consumer" right is often an object of criticism from advocates and Europeans who regard privacy as a human right.[124] But both COPRA and USCDPA, unlike some other bills, refer to "individuals," not "consumers." In this light, there is no need to draw that fight by referring to legislation as a consumer bill.

Although COPRA and USCDPA both use "data" in their titles, both define this term as "information" that is linked or linkable to an "individual." Data by itself is just digits. It is information that can be derived from data that becomes significant for privacy purposes. It is information that provides value to the covered entities that collect or share the data, and information is what gives individual an abiding interest in the data.

Different terms in the title would recognize that individuals have a privacy interest in all information—not merely online information—regardless of how it is collected or transmitted. Thus, we would choose to call a baseline privacy bill the "Information Privacy Act."

E. Legislative Findings

Legislative findings are frequently overlooked in legislative drafting. The majority of privacy bills or draft bills—including COPRA, USCDPA, and CDPSA—have not included legislative findings thus far.

Such findings can help increase congressional and public support for a bill and build an unassailable record of congressional intent to guide interpretation of the statute.[125] Such a record will be especially important for privacy legislation, which is likely to face constitutional litigation—such as First Amendment limitations or Article III standing questions under *Sorrell v. IMS Health, Inc*. and *Spokeo, Inc. v. Robinson*—and can express the importance of privacy to the world.[126]

With these considerations in mind, a privacy law should contain legislative findings. At Brookings, we have an ongoing project to analyze the appropriate content of such legislative findings.

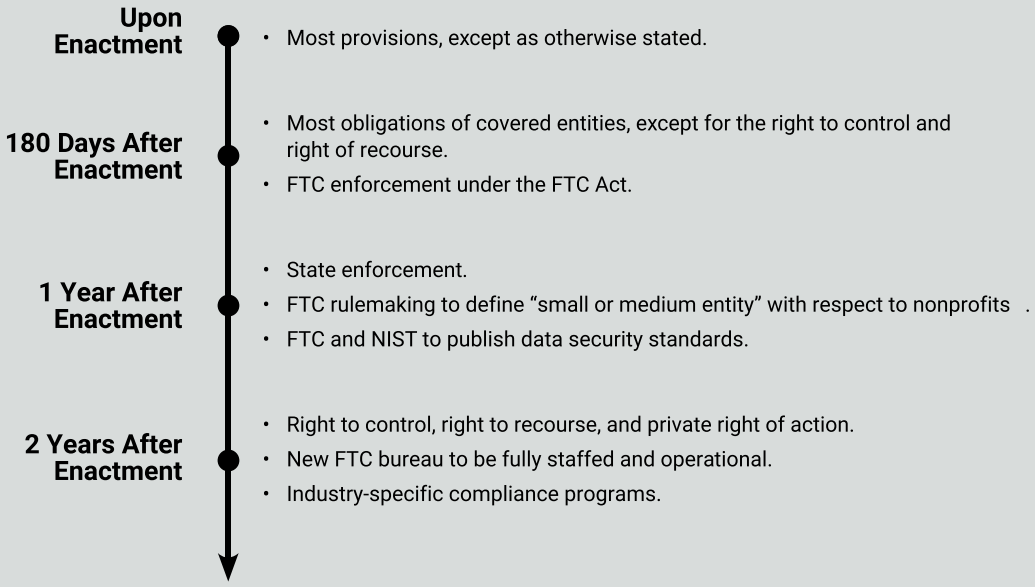
F. Effective Dates

The effective date of legislation must balance multiple considerations, including the need to allow covered entities enough time for compliance, versus the degree of urgency for the act to become effective. As we have discussed in this report, some of the obligations proposed in privacy legislation entail significant planning for compliance programs, business processes, and public interfaces.

In current legislative proposals, effective dates have varied. COPRA would take effect 180 days after enactment, while USCDPA would be effective two years following enactment. Meanwhile, CDPSA would enter into force one year after enactment—except the bill's preemption provision, which would take effect immediately.

We recommend tiered effective dates, with certain provisions taking effect at different times to allow time not only for compliance, but also for the FTC to manage rulemakings and guidance necessary to inform implementation of some provisions. In general, we suggest that federal privacy legislation take

Figure 2: Timeline of Effective Dates



effect immediately upon enactment, which would bring FTC rulemaking and staffing authority and the federal preemption of inconsistent state laws into force immediately. To allow time for compliance, most obligations for covered entities should become effective 180 days after enactment. We recommend, however, that the "right to control" and "right to recourse" become effective two years after enactment because both call for FTC rulemakings, which we believe should be completed 18 months after enactment to allow the agency to staff up and complete rulemaking with earlier deadlines.

Just as CCPA provided that enforcement would not begin until six months after coming into effect, we suggest a grace period for enforcement actions: six months after the effective date for FTC or state actions and two years for private actions.

Conclusion

The recommendations and analysis in this report frame the kinds of compromises it will take to pass federal privacy legislation that would give individuals stronger, more consistent expectations for how organizations use personal information, while also giving industry clear national guidance on what it needs to do to protect privacy and security. Last year's gridlock on the Washington Privacy Act (WPA) shows that state legislation is no slam dunk for either side of the debate and that bipartisan federal privacy legislation will take compromise. In Washington State—a fairly liberal state with a Democrat-controlled state house—efforts to resolve the private right of action failed, and WPA ultimately went down to defeat after both business interests and advocacy groups dug in.[127] If the same thing happens in Washington, D.C., any window of opportunity to pass federal privacy legislation is likely to reach a similar end.

Thus, for the federal privacy debate to move forward, stakeholders will need to find middle ground on a range of issues. Perhaps the suggestions here can help.

About the Authors

Cameron F. Kerry is the Ann R. and Andrew H. Tisch Distinguished Visiting Fellow at The Brookings Institution. In addition to his work at Brookings, Kerry is also a visiting scholar with the MIT Media Lab. Previously, he served as General Counsel and Acting Secretary of the U.S. Department of Commerce, where he led the Obama administration's work on consumer privacy, including the Consumer Privacy Bill of Rights. He has also spent time in private practice as a litigator and regulatory lawyer.

John B. Morris, Jr. is a non-resident senior fellow at The Brookings Institution. Until May 2019, Morris served—under two presidential administrations—as a career member of the Senior Executive Service at the National Telecommunications and Information Administration of the U.S. Department of Commerce. He led NTIA's Office of Policy Analysis & Development, where he worked on legislation and other activities implementing the Consumer Privacy Bill of Rights. Previously, Morris served as General Counsel of the Center for Democracy & Technology.

Caitlin T. Chin is a research assistant at The Brookings Institution, where she analyzes policy issues and governance challenges related to information privacy, artificial intelligence, broadband, and antitrust. Previously, she completed the Google Public Policy Fellowship and Atlantic Media Fellowship programs and interned with Verizon's privacy policy office.

Nicol E. Turner Lee is a fellow at The Brookings Institution. At Brookings, she speaks and writes on the intersection of race, wealth, and technology within the context of civic engagement, criminal justice, and economic development. Previously, she worked at the Multicultural Media, Telecom, and Internet Council and the Joint Center for Political and Economic Studies.

Acknowledgments

We would like to thank our Brookings colleagues for their support of *The Privacy Debate* initiative since its inception, including Darrell West, Leti Davalos, Louis Serino, Jessica Harris, Jack Karsten, Courtney Dunakin, Emily Perkins, Brigitte Brown, India English, Raj Karan Gambhir, Marla Odell, Bhaargavi Ashok, and Lia Newman.

We are additionally grateful to Stacey Gray, Pollyanna Sanderson, and John Verdi at the Future of Privacy Forum for technical assistance on some of the difficult issues. Finally, we acknowledge the approximately 175 individuals—from academia, civil society, government, and industry—who have offered valuable feedback, insight, and reality checks in roundtables, public events, and private conversations. Because many of these conversations have been off-the-record or under the Chatham House rule, we do not identify them.

Disclosure

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. The conclusions and recommendations of any Brookings publication are solely those of its author(s), and do not reflect the views of the Institution, its management, or its other scholars. The following companies mentioned in this report provide support to The Brookings Institution: Apple, AT&T, Comcast, Facebook, Google, Microsoft, and Verizon. The findings, interpretations, and conclusions in this report are not influenced by any donation.

Endnotes

1 Consumer Online Privacy Rights Act of 2019, S. 2868, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968/text; "Fact Sheet: Chairman Wicker's Discussion Draft The United States Consumer Data Privacy Act," Senate Committee on Commerce, Science, and Transportation, December 3, 2019, https://www.commerce.senate.gov/2019/12/chairman-wicker-s-discussion-draft-the-united-states-consumer-data-privacy-act.

2 Cameron F. Kerry, "Game on: What to make of Senate privacy bills and hearing," The Brookings Institution, *TechTank*, December 3, 2019, https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/.

3 Margaret Harding McGill, "Federal privacy legislation shows signs of life in House," *Axios*, December 19, 2019, https://www.axios.com/federal-privacy-legislation-shows-signs-of-life-in-house-e519ac0b-b512-47e1-8c84-aaf57d4144cf.html; Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3456/text.

4 Natasha Singer and Choe Sang-Hun, "As coronavirus surveillance escalates, personal privacy plummets," *The New York Times*, March 23, 2020, https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html.

5 Cameron F. Kerry, "Why protecting privacy is a losing game today—and how to change the game," The Brookings Institution, July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

6 "Policy principles for a federal data privacy framework in the United States," Opening Statements of Chairman Roger Wicker and Ranking Member Maria Cantwell in the in the Senate Committee on Commerce, Science, and Transportation, February 27, 2019, https://www.commerce.senate.gov/2019/2/policy-principles-for-a-federal-data-privacy-framework-in-the-united-states.

7 Woodrow Hartzog, "Policy principles for a federal data privacy framework in the United States," Testimony before the Senate Committee on Commerce, Science, and Transportation, February 27, 2019, https://www.commerce.senate.gov/services/files/8B9ADFCC-89E6-4DF3-9471-5FD287051B53.

8 Private Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u–4, https://www.law.cornell.edu/uscode/text/15/78u-4.

9 "EU-U.S. Privacy Shield: Third review welcomes progress while identifying steps for improvement," European Commission, October 23, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134.

10 Kelly Servick, "COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work?" *Science Magazine*, May 21, 2020, https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how.

11 Cynthia J. Larose, "Alabama becomes 50th state to enact data breach notification law," Mintz Levin, April 3, 2018, https://www.mintz.com/insights-center/viewpoints/2826/2018-04-alabama-becomes-50th-state-enact-data-breach-notification.

12 *The Privacy Debate,* The Brookings Institution, https://www.brookings.edu/project/the-privacy-debate/.

13 Caitlin Chin and Marla Odell, "Highlights: Where stakeholders fall in the privacy debate," The Brookings Institution, *TechTank*, September 17, 2019, https://www.brookings.edu/blog/techtank/2019/09/17/highlights-where-stakeholders-fall-in-the-privacy-debate/.

14 *New State Ice Co. v. Liebmann*, 285 U.S. 262 (1932), https://www.law.cornell.edu/supremecourt/text/285/262#writing-type-1-SUTHERLAND.

15 Chris Conley, "California leads on electronic privacy. Other states must follow," *American Civil Liberties Union* (blog), October 13, 2015, https://www.aclu.org/blog/privacy-technology/internet-privacy/california-leads-electronic-privacy-other-states-must.

16 Dan Clark, "In-house counsel say preemption is important for federal data privacy law," *Law.com*, December 5, 2019, https://www.law.com/corpcounsel/2019/12/05/in-house-counsel-say-preemption-is-important-for-federal-data-privacy-law/?slreturn=20200426155201; Peter Swire, "Privacy legislation series: Understanding federal preemption," Future of Privacy Forum, December 19, 2019, https://www.youtube.com/watch?v=71GgQw3hwUk&feature=youtu.be.

17 Cable Communications Policy Act of 1984, 47 U.S.C. § 556, https://www.law.cornell.edu/uscode/text/47/556.

18 Jesse Merriam, "Preemption as a consistency doctrine," *William and Mary Bill of Rights Journal,* Volume 25, Issue 3, 2017, https://scholarship.law.wm.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1815&context=wmborj.

19 Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681, https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf.

20 Sarah Bouchard, "Credit card industry steps up lobbying," *Roll Call*, July 22, 2003, https://www.rollcall.com/2003/07/22/credit-card-industry-steps-up-lobbying/.

21 Mark Malonzo, "Protecting privacy requires private rights of action, not forced arbitration," Public Knowledge (blog), August 6, 2019, https://www.publicknowledge.org/blog/protecting-privacy-requires-private-rights-of-action-not-forced-arbitration/.

22 Rebecca Kern and Daniel R. Stoller, "Bipartisan privacy talks split with second Senate GOP bill (1)," *Bloomberg Law,* March 12, 2020, https://news.bloomberglaw.com/privacy-and-data-security/bipartisan-privacy-talks-split-as-second-senate-gop-bill-arrives.

23 Joseph F. Yenouskas and Levi W. Swank, "Emerging legal issues in data breach class actions," *Business Law Today* (blog), July 13, 2018, https://www.americanbar.org/groups/business_law/publications/blt/2018/07/data-breach/.

24 Samuel Warren and Louis Brandeis, "The right to privacy," *Harvard Law Review* Vol. IV No. 5, December 15, 1890, https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

25 Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681, https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf.

26 The Privacy Act 5 U.S.C. § 552a(g), https://www.law.cornell.edu/uscode/text/5/552a; The Right to Financial Privacy Act, 12 U.S.C. § 3417, https://www.law.cornell.edu/uscode/text/12/3417; The Cable Communications Policy Act, 47 U.S.C. § 551(f), https://www.law.cornell.edu/uscode/text/47/551; The Electronic Communications Privacy Act, 18 U.S.C. § 2707, https://www.law.cornell.edu/uscode/text/18/2707; The Video Privacy Protection Act, 18 U.S.C. § 2710(c), https://www.law.cornell.edu/uscode/text/18/2710; The Telephone Consumer Protection Act 47 U.S.C. § 227(b)(3), https://www.law.cornell.edu/uscode/text/47/227.

27 William L. Prosser, "Privacy," *California Law Review* 48, no. 3, 1960: 383-423, doi:10.2307/3478805.

28 Scott Delacourt, "Abusive robocalls and how we can stop them," Testimony before the Senate Committee on Commerce, Science, and Transportation, April 18, 2018, https://www.commerce.senate.gov/services/files/7b94454d-d7c5-4231-ad32-e53f8080685f.

29 Brian Kint, "Case update: *Wakefield v. ViSalus, Inc,*" Cozen O'Connor, June 27, 2019, https://www.jdsupra.com/legalnews/case-update-wakefield-v-visalus-inc-21856/.

30 "The Privacy Advisor Podcast special edition: Edelson on his firms' $925M privacy class-action win," *IAPP,* April 15, 2019, https://iapp.org/news/a/the-privacy-advisor-podcast-edelson-on-his-924m-privacy-class-action-win/.

31 "History of the ICO," Information Commissioner's Office, January 23, 2019, https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/.

32 In 1992, the Supreme Court ruled that plaintiffs must establish an "injury in fact" that is "concrete and particularized" in order to meeting standing requirements under Article III of the Constitution. *See: Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992), https://www.law.cornell.edu/supremecourt/text/504/555.

33 *Spokeo, Inc. v. Robins*, 578 U.S. ___, 136 S. Ct. 1540 (2016), https://www.supremecourt.gov/opinions/15pdf/13-1339dif_3m92.pdf.

34 California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.150 (2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121.

35 The Massachusetts Consumer Protection Law, Mass. Gen. Laws Chapter 93A, https://malegislature.gov/laws/generallaws/parti/titlexv/chapter93a.

36 "Rule 68. Offer of Judgment," *Legal Information Institute*, May 15, 2020, https://www.law.cornell.edu/rules/frcp/rule_68.

37 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/4978.

38 Private Securities Litigation Reform Act of 1995, 15 U.S.C. § 78u–4, https://www.law.cornell.edu/uscode/text/15/78u-4.

39 Right to Financial Privacy Act of 1978, 12 U.S.C. § 3416, https://www.law.cornell.edu/uscode/text/12/chapter-35.

40 Data Care Act of 2018, S.3744, 115th Cong. § 3 (2018), https://www.congress.gov/bill/115th-congress/senate-bill/3744.

41 "Revised Common Rule," HHS Office for Human Research Protections, https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html.

42 "Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy," The White House, February 23, 2012, https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

43 House Committee on Energy and Commerce, Bipartisan Staff Discussion Draft, 116th Cong. § 6(b) (2019), https://www.axios.com/federal-privacy-legislation-shows-signs-of-life-in-house-e519ac0b-b512-47e1-8c84-aaf57d4144cf.html.

44 Helen Nissenbaum, "Privacy as contextual integrity," *Washington Law Review*, 2004, https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf.

45 Woodrow Hartzog, "Privacy's blueprint: The battle to control the design of new technologies," *Harvard University Press*, 2018.

46 Restatement of the Law, Second, Torts, § 652 (1977), https://cyber.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm.

47 Cameron F. Kerry, "Why protecting privacy is a losing game today—and how to change the game," The Brookings Institution, July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

48 Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner, "Americans and privacy: Concerned, confused and feeling lack of control over their personal information," *Pew Research Center: Internet, Science & Tech* (blog), November 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

49 Alan F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, Volume 25, Issue 1, 1968, https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20.

50 Drew Harwell, "Facebook, longtime friend of data brokers, becomes their stiffest competition," *The Washington Post,* March 29, 2019, https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/facebook-longtime-friend-of-data-brokers-becomes-their-stiffest-competition/.

51 Pam Dixon, "What information do data brokers have on consumers?" Testimony before the Senate Committee on Commerce, Science, and Transportation, December 18, 2018, https://www.worldprivacyforum.org/2013/12/testimony-what-information-do-data-brokers-have-on-consumers/.

52 "FTC to study data broker industry's collection and use of consumer data," Federal Trade Commission, December 18, 2012, https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data; Natasha Singer, "Acxiom lets consumers see data it collects, *The New York Times*, September 4, 2013, https://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html.

53 Consumer Data Protection Act, H.R. 4544, 115th Cong. (2018), https://www.congress.gov/bill/115th-congress/house-bill/4544.

54 "Big data: Seizing opportunities, preserving values," The White House, February 2015, https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf.

55 Megan Smith, DJ Patil, and Cecilia Muñoz, "Big risks, big opportunities: The intersection of big data and civil rights," The White House, May 4, 2016, https://obamawhitehouse.archives.gov/blog/2016/05/04/big-risks-big-opportunities-intersection-big-data-and-civil-rights; "Big data: A tool for inclusion or exclusion?" Federal Trade Commission, January 2016, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.

56 Cameron F. Kerry, "Protecting privacy in an AI-driven world," The Brookings Institution, February 10, 2020, https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.

57 Alexandra George, "Thwarting bias in AI systems," Carnegie Mellon University, College of Engineering, December 11, 2018, https://engineering.cmu.edu/news-events/news/2018/12/11-datta-proxies.html.

58 Caitlin Chin and Bhaargavi Ashok, "Highlights: Addressing fairness in the context of artificial intelligence," The Brookings Institution, *TechTank*, November 18, 2019, https://www.brookings.edu/blog/techtank/2019/11/18/highlights-addressing-fairness-in-the-context-of-artificial-intelligence/.

59 Latanya Sweeney, "Discrimination in online ad delivery," SSRN Scholarly Paper, January 28, 2013, https://doi.org/10.2139/ssrn.2208240; Jordan Pearson, "How big data could discriminate," *Vice*, September 16, 2014, https://www.vice.com/en_us/article/d73x7v/why-the-federal-trade-commission-thinks-big-data-could-be-discriminatory.

60 Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e, https://www.law.cornell.edu/uscode/text/42/2000e; Americans with Disabilities Act of 1990, 42 U.S.C. § 12101, et seq., https://www.law.cornell.edu/uscode/text/42/12101.

61 Michael Kearns and Aaron Roth, "Ethical algorithm design should guide technology regulation," The Brookings Institution, January 13, 2020, https://www.brookings.edu/research/ethical-algorithm-design-should-guide-technology-regulation/.

62 Cameron F. Kerry, "Protecting privacy in an AI-driven world," The Brookings Institution, February 10, 2020, https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.

63 Caitlin Chin, "Assessing employer intent when AI hiring tools are biased," The Brookings Institution, December 13, 2019, https://www.brookings.edu/research/assessing-employer-intent-when-ai-hiring-tools-are-biased/.

64 Steve Lohr, "If algorithms know all, how much should humans help?" *The New York Times*, April 6, 2015, https://www.nytimes.com/2015/04/07/upshot/if-algorithms-know-all-how-much-should-humans-help.html.

65 Stanley Augustin, "Lawyers' Committee for Civil Rights Under Law and Free Press Action release proposed 'Online Civil Rights and Privacy Act' to combat data discrimination," Lawyers' Committee, March 11, 2019, https://lawyerscommittee.org/lawyers-committee-for-civil-rights-under-law-and-free-press-action-release-proposed-online-civil-rights-and-privacy-act-to-combat-data-discrimination/.

66 Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e, https://www.law.cornell.edu/uscode/text/42/2000e-2.

67 Genetic Information Non-Discrimination Act of 2008, 42 U.S.C. § 300gg-51 et seq., https://www.law.cornell.edu/uscode/text/42/300gg-51.

68 Fair Housing Act of 1968, 42 U.S.C. § 3601-3619 and 3631, https://www.law.cornell.edu/uscode/text/42/chapter-45.

69 David Hudson, "President Obama signs a new executive order to protect LGBT workers," The White House, July 21, 2014, https://obamawhitehouse.archives.gov/blog/2014/07/21/president-obama-signs-new-executive-order-protect-lgbt-workers; *David Baldwin v. Anthony Foxx*, Appeal No. 012v0133080, 2015 WL 4397641 (E.E.O.C. 2015), https://www.eeoc.gov/sites/default/files/migrated_files/decisions/0120133080.pdf; *Obergefell v. Hodges*, 576 U.S. 644 (2015), https://www.supremecourt.gov/opinions/14pdf/14-556_3204.pdf.

70 *Macy v. Holder*, No. 0120120821, 2012 WL 1435995 (E.E.O.C. 2012), https://www.eeoc.gov/sites/default/files/migrated_files/decisions/0120120821%20Macy%20v%20DOJ%20ATF.txt; Adam Liptak and Jeremy W. Peters, "Supreme Court considers whether Civil Rights Act protects LGBT workers," *The New York Times*, November 7, 2019, https://www.nytimes.com/2019/10/08/us/politics/supreme-court-gay-transgender.html.

71 Civil Rights Act of 1991, 42 U.S.C. § 1997a, https://www.eeoc.gov/statutes/civil-rights-act-1991.

72 John Villasenor and Virginia Foggo, "Why a proposed HUD rule could worsen algorithm-driven housing discrimination," The Brookings Institution, *TechTank*, April 16, 2020, https://www.brookings.edu/blog/echtank/2020/04/16/why-a-proposed-hud-rule-could-worsen-algorithm-driven-housing-discrimination/.

73 *Summers v. Tice* 33 Cal. 2d 80, 199 P.2d 1 (Cal. 1948), https://scocal.stanford.edu/opinion/summers-v-tice-26161.

74 Cameron F. Kerry, "Protecting privacy in an AI-driven world," The Brookings Institution, February 10, 2020, https://www.brookings.edu/research/protecting-privacy-in-an-ai-driven-world/.

75 General Data Protection Regulation, Article 22 (2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

76 Algorithmic Accountability Act of 2019, S.1108, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1108.

77 Section 444 of the General Education Provisions Act, *i.e.*, Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, https://www.law.cornell.edu/uscode/text/20/1232g; Jeffrey Selingo, "Colleges Use Predictive Data, Analytics to Find Students," *The Atlantic*, April 11, 2017, https://www.theatlantic.com/education/archive/2017/04/how-colleges-find-their-students/522516/.

78 Open Internet Order, 80 FR 19737 (2015), https://www.fcc.gov/document/fcc-releases-open-internet-order; Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, 81 FR 87274 (2017), https://www.fcc.gov/document/fcc-releases-rules-protect-broadband-consumer-privacy.

79 "The big picture: Comprehensive online data collection," Panelist Comments in Federal Trade Commission Workshop, 2012, https://www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf.

80 Kimberly Kindy, "How Congress dismantled internet privacy rules," *The Washington Post*, May 30, 2017, https://www.washingtonpost.com/politics/how-congress-dismantled-federal-internet-privacy-rules/2017/05/29/7ad06e14-2f5b-11e7-8674-437ddb6e813e_story.html.

81 Mehreen Khan, "Companies face high cost to meet new EU data protection rules," *Financial Times*, November 19, 2017, https://www.ft.com/content/0d47ffe4-ccb6-11e7-b781-794ce08b24dc; David Roland-Holst et al., "Standardized regulatory impact assessment: California Consumer Privacy Act of 2018 Regulations," Berkeley Economic Advising and Research, LLC, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.

82 Edward Moyer, "Facebook whistleblower's startup reportedly had access to data too," *CNET*, March 28, 2018, https://www.cnet.com/news/facebook-cambridge-analytica-whistleblowers-start-up-had-data-access-too/; "FTC approves final order settling charges against flashlight app creator," Federal Trade Commission, April 9, 2014, https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app.

83 "Cases and Proceedings; Cases Tagged with Privacy and Security + Consumer Privacy + Data Security + Identity Theft," Federal Trade Commission, https://www.ftc.gov/enforcement/cases-proceedings/terms/245%2B247%2B249%2B262.

84 "Records, computers, and the rights of citizens," U.S. Department of Health & Human Services, July 1, 1973, https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

85 Notification of Risk to Personal Data Act of 2003, S. 1350, 108th Cong. (2003), https://www.judiciary.senate.gov/imo/media/doc/02-04-14FeinsteinStatement.pdf; Rachel German, "What are the chances for a federal breach notification law?" University of Texas at Austin, Center for Identity, https://identity.utexas.edu/id-experts-blog/what-are-the-chances-for-a-federal-breach-notification-law.

86 Barack Obama, "Remarks by the President in State of the Union Address," The White House, January 20, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/01/20/remarks-president-state-union-address-January-20-2015; Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. (2015), https://www.congress.gov/bill/114th-congress/house-bill/1704.

87 Teresa Troester Falk, "The concept of 'accountability' as a privacy and data protection principle," *CPO Magazine*, February 19, 2016, https://www.cpomagazine.com/data-privacy/concept-accountability-privacy-data-protection-principle/.

88 Sarbanes-Oxley Act of 2002, 15 U.S.C. § 7241, https://www.law.cornell.edu/uscode/text/15/7241.

89 "SEC adopts statement and interpretive guidance on public company cybersecurity disclosures," Securities and Exchange Commission, February 21, 2018, https://www.sec.gov/news/press-release/2018-22.

90 Kurt Mueffelmann, "Uber's privacy woes should serve as a cautionary tale for all companies," *Wired*, January 23, 2015, https://www.wired.com/insights/2015/01/uber-privacy-woes-cautionary-tale/.

91 Aaron Tilley and Robert McMillan, "Zoom CEO: 'I really messed up' on security as coronavirus drove video tool's appeal," *The Wall Street Journal*, April 4, 2020, https://www.wsj.com/articles/zoom-ceo-i-really-messed-up-on-security-as-coronavirus-drove-video-tools-appeal-11586031129.

92 Letter from Marc Rotenberg and Catriona Fitzgerald to Senators Roger Wicker and Maria Cantwell, December 3, 2019, https://epic.org/testimony/congress/EPIC-SCOM-LegislativePrivacyProposals-Dec2019.pdf; "The U.S. urgently needs a data protection agency," Electronic Privacy Information Center, https://epic.org/dpa/.

93 Data Protection Act of 2020, S. 3300, 116th Cong. (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3300/text.

94 Chris Hoofnagle, Woodrow Hartzog, and Daniel Solove, "The FTC can rise to the privacy challenge, but not without help from Congress," The Brookings Institution, *TechTank*, August 8, 2019, https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/.

95 Caitlin Chin and Marla Odell, "Highlights: Commissioners discuss the future of the FTC's role in privacy," The Brookings Institution, *TechTank*, November 5, 2019, https://www.brookings.edu/blog/techtank/2019/11/05/highlights-commissioners-discuss-the-future-of-the-ftcs-role-in-privacy/; Jack Karsten, "Pursuing a harms-based approach to privacy and antitrust regulation," The Brookings Institution, *TechTank*, March 27, 2019, https://www.brookings.edu/blog/techtank/2019/03/27/pursuing-a-harms-based-approach-to-privacy-and-antitrust-regulation/.

96 Federal Trade Commission Act of 1914, 15 U.S.C. § 45, https://www.law.cornell.edu/uscode/text/15/45.

97 "FTC approves final settlement with Facebook." Federal Trade Commission, August 10, 2012. https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.

98 Federal Trade Commission Act of 1914, 15 U.S.C. § 45. https://www.law.cornell.edu/uscode/text/15/45.

99 According to the U.S. Small Business Administration, there are 30.2 million small businesses in the United States, representing 99.9 percent of U.S. companies. *See:* "2018 Small Business Profile," U.S. Small Business Administration, Office of Advocacy, https://www.sba.gov/sites/default/files/advocacy/2018-Small-Business-Profiles-US.pdf.

100 "History of the ICO," Information Commissioner's Office, January 23, 2019, https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/.

101 Julie Brill, "Examining legislative proposals to protect consumer data privacy," Testimony before the Senate Committee on Commerce, Science, and Transportation, December 4, 2019, https://www.commerce.senate.gov/2019/12/examining-legislative-proposals-to-protect-consumer-data-privacy.

102 Pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015, the FTC annually adjusts maximum civil penalties to account for inflation. In 2020, the maximum civil penalty changed from $42,530 to $43,280 per day for violations of Section 5(l), 5(m)(1)(A), and 5(m)(1)(B) of the FTC Act. *See*: "FTC publishes inflation-adjusted civil penalty amounts," Federal Trade Commission, January 13, 2020, https://www.ftc.gov/news-events/press-releases/2020/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts.

103 Federal Trade Commission Act of 1914, 15 U.S.C. § 57a, https://www.law.cornell.edu/uscode/text/15/57a.

104 Cameron F. Kerry and Daniel Weitzner, "Rulemaking and its discontents: Moving from principle to practice in federal privacy legislation," The Brookings Institution, *TechTank*, June 5, 2019, https://www.brookings.edu/blog/techtank/2019/06/05/rulemaking-and-its-discontents-moving-from-principle-to-practice-in-federal-privacy-legislation/.

105 *Id.*

106 *Id.*

107 Cameron F. Kerry, "Breaking down proposals for privacy legislation: How do they regulate?" The Brookings Institution, March 8, 2019, https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/.

108 "U.S. Chamber releases model privacy legislation, urges Congress to pass a federal privacy law," U.S. Chamber of Commerce, February 13, 2019, https://www.uschamber.com/press-release/us-chamber-releases-model-privacy-legislation-urges-congress-pass-federal-privacy-law; "Internet Association proposes privacy principles for a modern national regulatory framework," Internet Association, September 12, 2018, https://internetassociation.org/internet-association-proposes-privacy-principles-for-a-modern-national-regulatory-framework/.

109 Cameron F. Kerry and Caitlin Chin, "Hitting refresh on privacy policies: Recommendations for notice and transparency," The Brookings Institution, *TechTank*, January 6, 2020, https://www.brookings.edu/blog/techtank/2020/01/06/hitting-refresh-on-privacy-policies-recommendations-for-notice-and-transparency/.

110 Julie Brill, "GDPR's first anniversary: A year of progress in privacy protection," Microsoft, *On the Issues Blog*, May 20, 2019, https://blogs.microsoft.com/on-the-issues/2019/05/20/gdprs-first-anniversary-a-year-of-progress-in-privacy-protection/.

111 COPRA (Section 2(11)) and USCDPA (Section 2(14)) use "derived data" and "inferred data" as respective terms for inferences or predictions about individuals drawn from covered data.

112 The Data Privacy Lab at Harvard University has documented flows of personal information, including mobile app and health data. *See:* theDataMap, available at: https://thedatamap.org/index.php.

113 "11. Dispute Resolution and Enforcement (d) - (e)," Privacy Shield Framework, https://www.privacyshield.gov/article?id=11-Dispute-Resolution-and-Enforcement-d-e.

114 Washington Privacy Act of 2019, S.B. 5376, H.R. 1854, Washington State Legislature (2019), https://app.leg.wa.gov/billsummary?BillNumber=5376&Initiative=false&Year=2019.

115 "EU-U.S. Privacy Shield: Third Review Welcomes Progress While Identifying Steps for Improvement," European Commission, October 23, 2019, https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6134.

116 "Records, computers, and the rights of citizens," U.S. Department of Health & Human Services, July 1, 1973, https://aspe.hhs.gov/report/records-computers-and-rights-citizens.

117 The Gramm-Leach Bliley Act is responsible for the annual notices that U.S. individuals receive from financial services companies. Financial Modernization Act of 1999, i.e., Gramm-Leach-Bliley Act, 15 U.S.C. § 23 6801 et seq., https://www.law.cornell.edu/uscode/text/15/6801.

118 Aleecia M. McDonald and Lorrie Faith Cranor, "The cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society*, 2008, https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf.

119 Cameron F. Kerry, "Why protecting privacy is a losing game—and how to change the game," The Brookings Institution, July 12, 2018, https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

120 *Nomi Technologies, Inc., In the Matter Of*, Federal Trade Commission, September 3, 2015, https://www.ftc.gov/enforcement/cases-proceedings/132-3251/nomi-technologies-inc-matter; *Toysmart.Com, LLC, and Toysmart.Com, Inc.*, Federal Trade Commission, July 21, 2000, https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc; *Facebook, Inc., In the Matter Of.,* Federal Trade Commission, April 28, 2020, https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc.

121 Nitasha Tiku, "Why your inbox is crammed full of privacy policies," *Wired*, May 24, 2018, https://www.wired.com/story/how-a-new-era-of-privacy-took-over-your-email-inbox/.

122 Aaron Smith, "Half of online Americans don't know what a privacy policy is," *Pew Research Center,* December 4, 2014, https://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/.

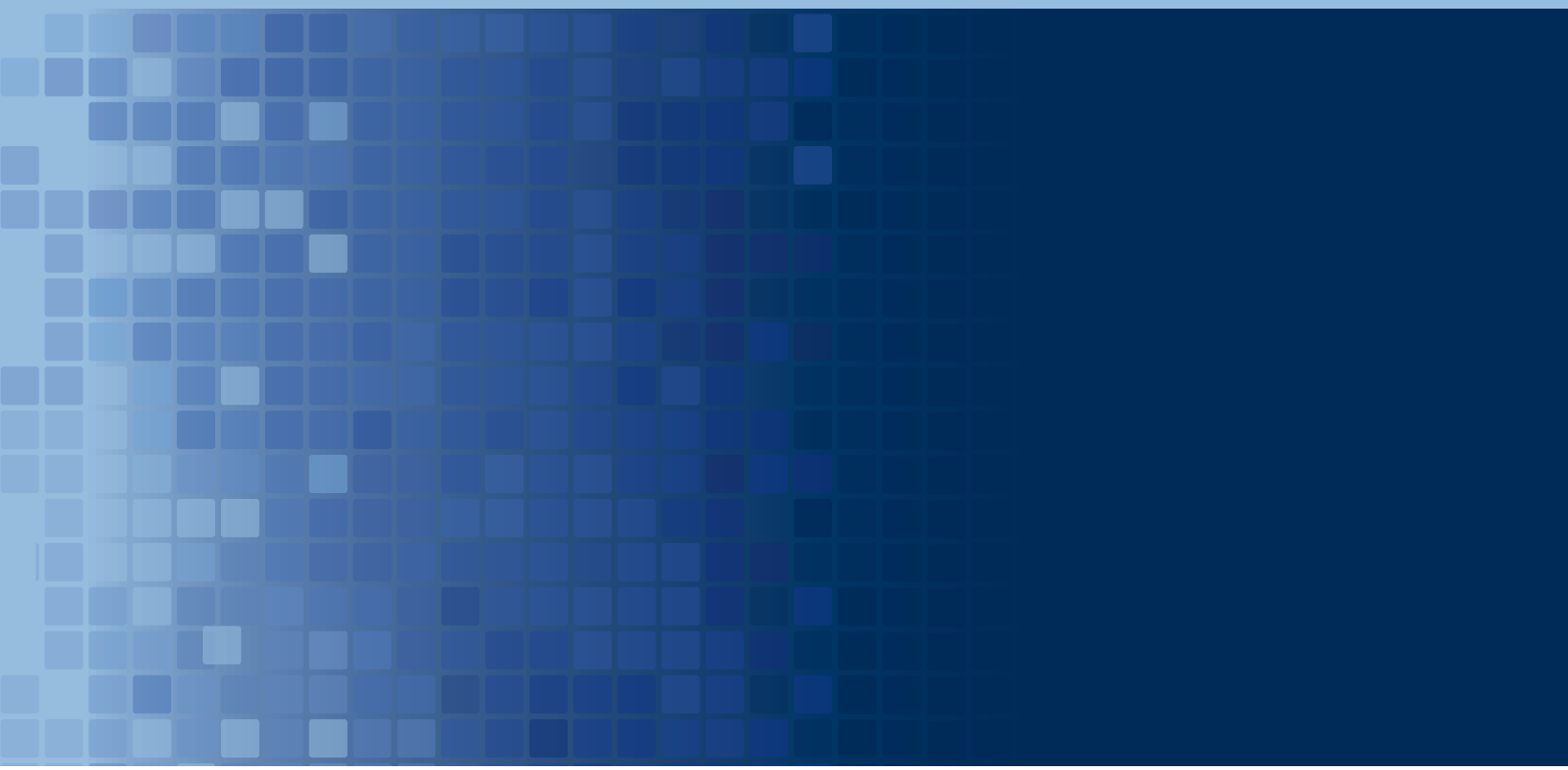
123 Online Privacy Act of 2019, H.R. 4978, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/house-bill/4978.

124 Paul M. Schwartz and Karl-Nikolaus Peifer, "Structuring international data privacy law," https://www.law.berkeley.edu/wp-content/uploads/2019/10/Schwartz-Intl-Data-Privacy-Law-21.pdf.

125 Jarrod Shobe, "Enacted legislative findings and purposes," *University of Chicago Law Review*, Vol. 86, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3387593.

126 *Sorrell v. IMS Health, Inc.,* 564 U.S. 552 (2011), https://www.supremecourt.gov/opinions/10pdf/10-779.pdf; *Spokeo, Inc. v. Robins,* 578 U.S. ___, 136 S. Ct. 1540 (2016), https://www.supremecourt.gov/opinions/15pf/13-1339dif_3m92.pdf.

127 Jennifer Bryant, "Washington Privacy Act fails for second time," *IAPP,* March 13, 2020, https://iapp.org/news/a/washington-privacy-act-fails-for-second-time/.



Governance Studies
at BROOKINGS

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, D.C. 20036
Brookings.edu