Legal Backgrounder

Vol. 36 No. 1 January 22, 2021

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Wolf in Sheep's Clothing: The "Data Accountability and Transparency Act"

by Kirk Herath

When is a privacy bill not really a privacy bill? When it creates a new federal administrative agency authorized to issue broad rules and regulate the permissible use of all data with an eye toward reordering America's business interactions and financial instruments in more "equitable" ways.

Last June, Senator Sherrod Brown released a legislative proposal, the Data Accountability and Transparency Act of 2020, or "the Bill." The Senator's press release stated the Bill will "protect consumers' privacy from 'bad actors.'" It further proclaimed that the Bill would "end intrusive data collection by empowering consumers, enhance civil rights protections, and establish a new independent agency dedicated to protecting individual privacy rights." Many consumer and allied groups heartily applauded. Industry, however, was conspicuously silent.

Perhaps at the time of the Bill's release, most business groups saw it as political posturing from the ranking member of the U.S. Senate Committee on Banking, Housing, and Urban Affairs. With Senator Brown assuming the Committee Chair, however, the proposal, or at least the concepts contained therein, will now be taken far more seriously.

Senator Brown's proposal creates a new civil rights framework for regulating data that rejects the "consent" model for privacy. It places strict limits on the collection, use, and sharing of personal data and prohibits the use of personal data for "any" discriminatory purposes. This would seem to include heretofore "legally" permissible practices to risk-rate the price of certain products and services, particularly property and life insurance.

Senator Brown has boasted, "My proposal would change the fundamental framework of privacy in this country." Any observer would agree that it most certainly would change how data is used in the United States, but it would also likely increase costs and reduce many Americans' access to financial products and services.

The Bill rejects the notice-and-consent regime that is the centerpiece of current U.S. privacy law, both federally and in the states. Even the much-heralded set of California privacy laws, known as the California Consumer Privacy Act and the recently passed ballot initiative known as the California Privacy Reform Act, operate on a more or less consent basis. Senator Brown's bill would replace that system with a new paradigm to ostensibly limit data collection to a narrow set of permissible purposes. In addition, the Bill would:

- Ban the collection, use, or sharing of personal data unless specifically allowed by law.
- Prohibit the retention of data beyond the period strictly necessary to carry out a permissible purpose.
- Ban the use of facial recognition technology.

Kirk Herath, CIPP/US, CIPP/G, recently retired as Chief Privacy Officer from a Fortune 100 insurance and financial services company, and now teaches, writes, and consults on data privacy and cybersecurity issues. Mr. Herath was also a former Chairman of the Board of the International Association of Privacy Professionals and served on the first U.S. Department of Homeland Security Data Privacy and Integrity Advisory Council.

- Ban targeted advertising.
- Ban commingling of data even by affiliates of the same company.
- Prohibit the use of personal data to discriminate in housing, employment, credit, insurance, and public accommodations.
- Require anyone using automated decision systems to conduct testing on bias and disparate impact as well as to conduct risk assessments and accountability reports.
- Provide individuals with the rights of access, portability, transparency, deletion, accuracy, and correction, as well as the right to object to a claimed permissible purpose and to human review of automated decisions.
- Create a new, independent agency with rulemaking, supervisory, and enforcement authority, as well as the ability to issue civil penalties for violations of the Act, and a dedicated Office of Civil Rights to protect individuals from unfair, deceptive, abusive, and discriminatory practices. The agency would have broad rulemaking authority and could identify specific practices that it deems unfair, deceptive, abusive, or discriminatory.
- Establish a private right of action for individuals and empower state attorneys general. Importantly, stricter state laws are not preempted.
- Require CEO certification of compliance with the Act, which exposes CEOs and Boards of Directors to potential criminal and civil penalties.

The concepts enshrined in this Bill should be of significant concern to the insurance industry, or to any financial services company whose product pricing differentiates consumers by risk. Many of these new requirements go well beyond what any reasonable person would call "privacy," and they would effectively socialize many industries by prohibiting any risk differentiation through pricing.

Concerning insurance, the Bill presents significant challenges to the industry's conventional use and disclosure of personal data to sell, price, service, and administer insurance and financial products. Concerns about disparate impact and the use of algorithms to automate insurance underwriting are growing; however, there is no clear articulation from policymakers or regulators as to how disparate impact (*i.e.*, the unintentional discriminatory impact on a protected group) would be reasonably measured or identified, especially when insurers do not collect or use demographic data like race or ethnicity in the first place. This will:

1. shift the burden to insurers to disprove something that they may not be capable of factually disproving, and
2. narrow traditionally acceptable underwriting factors (*e.g.*, actuarially sound and correlative factors) based on shifting public policy that will result in more expensive insurance (and thus likely less coverage) and more inconvenient business-to-consumer interactions.

The paper will next address some of the specific consequences that would result if Congress adopted this or any similar proposal.

Impact on Insurance Underwriting. Under the Act, the Data Accountability and Transparency Agency can deem any underwriting or rating practice that results in a price difference or denial of insurance a privacy harm or discriminatory use of personal data. Such uses would be subject to new and possibly conflicting federal regulatory oversight, enforcement activity, and private civil litigation. How this framework would interact with existing state-based insurance regulation is unknown. Even when insurers base price differences among applicants on actuarially justified underwriting factors, they could violate the Act. Applicants who choose to opt out of automated, data-driven insurance underwriting could end up being priced higher, or denied more often, because of data-availability issues and process inefficiencies, which would likely (without

any overt attempt to discriminate along racial lines) lead to increased claims of bias or disparate impact.

Overly Broad Definition of Privacy Harm. The Bill defines "privacy harm" very broadly to include any adverse, or potentially adverse, consequence to an individual caused, in whole or in part, by the collection, use, or sharing of personal data, including: 1) an adverse outcome or decision related to insurance eligibility (*e.g.*, denial of an application or obtaining less favorable terms) and 2) discrimination or the otherwise unfair or unethical differential treatment with respect to an individual. A privacy harm, therefore, could arguably include the use of credit attributes, driving behaviors, or health information to rate insurance products to the extent they result in less favorable terms for the applicant.

Imprecise Definition of Unlawful Discrimination. The Bill prohibits discriminatory use of personal data. Discrimination can include contracting for insurance in a manner that discriminates against or otherwise makes the opportunity unavailable or offered on different terms based on a protected class or otherwise materially contributes to unlawful discrimination. Because the Bill does not precisely define "unlawful discrimination," and in fact permits the new Agency to interpret the term freely or create new interpretations through rulemaking, it potentially swallows up any generally acceptable risk factors insurers use to price insurance products. Taken to the extreme, this may result in socialized insurance pricing where everyone is charged the exact same rate and no pricing adjustments or eligibility determinations would be allowed based on individual risk factors or behavior. This would be the death knell of the insurance industry.

Private Right of Action Would Open the Litigation Floodgates. The bill would allow any person to bring a civil action against an organization in U.S. District Court alleging violations of the Act. A successful plaintiff may be awarded up to $1,000 per violation, per day; actual damages; punitive damages; and attorneys' fees/litigation costs. Trial lawyers must be salivating at the thought of such a treasure trove of civil actions based on broad and nebulous accusations.

Furthermore, a violation of the Bill or its regulations would constitute a "concrete and particularized injury in fact" to the affected individual, making it difficult for defendants to successfully have lawsuits dismissed even if the plaintiff suffered no actual damages. Affected individuals would have up to five years after discovering the violation to bring civil action.

Impossible Data-Governance Obligations. The Bill would limit an organization's ability to collect, use, and share personal data to a few permissible purposes. Organizations would be limited to using personal data only if strictly necessary in furtherance of a permissible purpose, such as providing a good or service requested by the consumer. However, even then, the Act would consider comingling of data from multiple services or applications to be an unlawful practice. The prohibition on comingling data potentially makes unlawful the combining of data collected through a car manufacturer's telematics program with data collected by the insurer to offer individualized pricing or customized products.

Even the use of public information curated by a third-party aggregator to prefill an application for insurance or file a claim could be unlawful commingling of personal data. Such an outcome would undermine efforts to automate consumer touchpoints (*e.g.*, entering data into applications or forms) by combining first and third-party data with artificial intelligence models to add convenience and efficiency to the consumer experience. The ubiquitous centralized customer-information databases that have become the hallmark of any efficient corporate or even governmental customer service model would become illegal overnight.

"Strictly Necessary" Data-Retention Trap. The Bill would require that data be deleted when it is no longer "strictly necessary" to carry out a permissible purpose. This could eliminate information needed for future analysis, as businesses look to more efficiently and effectively price or underwrite their products based on data-driven analysis. Accidentally or unintentionally keeping any data beyond a "strictly necessary" period would lead to individual lawsuits, class actions, and agency and state attorney-general enforcement actions. Again, how this would interact with existing federal and state insurance and financial services regulations is unknown.

ISBN 1056 3059

The Bill states that all collection, use, and sharing of personal data must be strictly necessary to carry out one or more permissible purposes listed in the Bill. This means that data governance must be in place throughout the entire data lifecycle to demonstrate that it was in fact collected, used, and shared only when strictly necessary to do so. Such systems of accountability are extremely expensive to implement and maintain and require strong data governance discipline. Businesses, particularly well-established ones, may need to undertake a costly and time-consuming redesign of their IT architecture to accommodate such governance.

Permissible Purpose. The Bill identifies several permissible purposes that are useful to the industry. However, the Bill limits the permissible collection of data related to providing goods and services to only when an individual has personally and intentionally requested them. This limitation likely hinders insurers' ability to underwrite insurance products intended for household purposes where data about additional insureds (or beneficiaries for life and investment products) may be collected without their knowledge or any direct interaction between them and the insurance company. The intentional-interaction requirement likely limits an insurer's ability to renew insurance coverage without policyholder authorization or to purchase prospect data from third-party data aggregators for legitimate marketing purposes. Also, the definition of personal data does not contain a commonly provided exclusion for publicly available information, which could prevent a business from even using that information.

Predictive Models. The Bill would impose new restrictions on the use of "automated decision systems" (*e.g.*, artificial intelligence or machine-learning algorithms) and would mandate that those who use decision-making algorithms provide transparency and accountability reports as directed by the Agency, but no less than annually. Additionally, individuals are entitled to human review of any automated decisions, which must be done by the business within 15 days of receiving a verified request. Creating such reports upon request for potentially every individual largely defeats the purpose of using automated tools to drive more efficient and consistent decision making. This would result in higher costs that are ultimately passed to the consumer. Automated decision systems must also be tested for bias or disparate impact on protected classes of individuals. While no one wishes bias or disparate impact to occur, testing for discrimination would require a methodology that does not currently exist and would require regulatory approval before it could be used. For example, insurers today do not collect factors like race or ethnicity, because these are not relevant factors in the underwriting process. However, in an odd twist of logic, testing for racial bias would probably result in the necessary collection of such information by insurers to determine unlawful racial impact.

*****

If enacted as proposed, the Bill would dramatically increase prices for all financial services products, particularly insurance, and reduce their availability. The law would reorder the U.S. economy, equalizing the price everyone pays for homeowners, auto, and life insurance, regardless of the underlying risks. It would penalize less risky individuals and disincentivize risk mitigation. Further, it would result in the dramatic elimination of most of the thousands of large, medium, and small insurers in the U.S. and millions of jobs. In their place would remain an exceedingly small number of mammoth insurance companies similar to what has happened to the U.S health insurance industry over the past 20 years.

Taking this scenario to its logical conclusion, why have private insurance companies at all? If the desire is to make all prices the same, with no need for competition, Congress might as well create a few new federal government-sponsored enterprises. They could be called the Federal Property & Casualty Assurance Corporation and the Federal National Life Assurance Corporation. Can anyone say Freddie Pac and Fannie Lac?

  ISBN 1056 3059