DURABLE PRIVACY LEGISLATION:

AN EVIDENCE-BASED PRIVACY LAW THAT WORKS FOR THE PEOPLE

JANE BAMBAUER[1]

Public demand for stronger privacy laws has reached a critical point, and congress is likely to pass sweeping, cross-technology and cross-industry privacy legislation for the first time in US history. This is an exciting juncture for information policy, but also a perilous one. Poorly constructed privacy laws can frustrate the interests of the people they are meant to protect.

This white paper explains why an evidence-based privacy law would not look like the GDPR or the CCPA, and offers the contours (and even model language) of a statutory scheme that would better serve the modern American consumer.[2]

WHAT DO WE KNOW ABOUT THE LIKELY EFFECTS OF THE GDPR AND CCPA?

The short-run effects of GDPR have not been good for the European economy. A recent study found evidence that GDPR caused a significant reduction in the quantity and size of venture capital investments across all sectors in Europe, costing millions of dollars per week in lost investments.[3] Start-ups and young firms lose out more often than established firms.[4] This is consistent with earlier theoretical work predicting that privacy compliance disproportionately burdens small firms, and tends to both deter innovation and move it from startups to established companies.[5] Some of these effects may be transitional as investors wait to see how GDPR is going to be interpreted and enforced, but there is little doubt that the transaction costs from securing consent or from failing to match services to customers will cause a drag on data-related innovations.

---

[1] Professor of Law, University of Arizona and Director, Program on Economics & Privacy at George Mason University Antonin Scalia Law School- janebambauer@email.arizona.edu https://law.arizona.edu/jane-bambauer

[2] This report draws heavily from my testimony and responses to questions at the Senate Judiciary Committee hearing on "The Likely Impact of the GDPR and the CCPA on Innovation and Consumer Welfare," held March 12, 2019.

[3] Jian Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment,* NBER WORKING PAPER NO. 25248 (2018).

[4] *Id.*

[5] James Campbell et al., *Privacy Regulation and Market Structure,* 24 J. ECON. & MGMT STRATEGY 47 (2015) (showing that identical compliance costs will disproportionately burden smaller firms); Silvana Krasteva et al., *The 80/20 Rule: Corporate Support for Innovation by Employees,* 38 INT. J. INDUS. ORG. 32 (2015) (using theoretical models to explore the development of innovations and finding that compliance costs both deter innovation and shift some of it into established firms).

> *"There is little doubt that the transaction costs from securing consent or from failing to match services to customers will cause a drag on data-related innovations."*

The CCPA is likely to have similar effects on the US economy. It is, in essence, a light version of the GDPR. Thus, we can expect a difficult transition period once the law comes into effect not only because of new substantive requirements like data deletion on request, but also because the law introduces new, vague concepts such as an anti-discrimination provision.[6]

This should give policymakers pause. The tech sector is the crown jewel of the U.S. economy. Not only is it the greatest source of productivity growth, but it also produces jobs and raises wages faster than any other industry.[7] And contrary to popular perception, there is more competition and less concentration in the tech sector than there was in the manufacturing sector during its heyday.[8] This is not to say that technology firms pose no risk to the distribution of resources, wealth and jobs in America. Rather, the creation of a right for consumers to control their personal data is a misguided and counterproductive solution for the existing and potential social problems we care most about.

The U.S. regulatory approach to privacy played a part in the development of the tech industry by permitting new and unexpected services to emerge, and by avoiding regulations where the harms were speculative or nonexistent. U.S. consumers are best served when regulators can use their expertise to identify and deter harmful and unduly risky endeavors that may on the surface seem harmless *and*, just as importantly, to permit low risk innovations that may on the surface seem creepy. Because the Federal Trade Commission has developed this expertise, Congress should continue to support their work with the clear mission to respond to concrete risks and harms.

TWO VIEWS OF PRIVACY: PROPERTY RULES AND LIABILITY RULES[9]

The GDPR, the CCPA, and most of the statutory privacy laws in this country and abroad incorporate versions of the Fair Information Practice Principles ("FIPPs"), originally developed in the 1973 HEW Report.[10] The core value of the FIPPs is a property-style right vested in the

---

[6] The California Consumer Privacy Act, Cal. Civ. Code §1798.125.

[7] Michael Mandel, *Competition and Concentration: How the Tech/Telecom/Ecommerce Sector Is Outperforming the Rest of the Private Sector,* PROGRESSIVE POLICY INSTITUTE POLICY MEMO (2018) at P12-13.

[8] Id. at P7-8. *See also* David Autor, *Why Are There Still So Many Jobs? The History and Future of Workplace Automation,* 29 J. ECON. PERSP. 3 (2015) (predicting that some of the thinning of the middle of the income distribution will reverse when we are further along in the transition to an AI-supported economy).

[9] Guido Calabresi & A. Douglas Melamed, Property Rules, Liability Rules, and Inalienability: One View of the Cathedral, 85 HARV. L. REV. 1089, 1122 (1972). For more information about the application of property and liability rules in the context of personal data, *see* Jane Yakowitz Bambauer, *The New Intrusion,* 88 NOTRE DAME L. REV. 205, 213-229 (2012).

[10] U.S. Dept. of Health, Educ. & Welfare, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973).

person described by data. Individuals are expected to have notice about the extent and nature of information collected about them, and a choice about whether to proceed. This notice and choice is designed to give individuals ultimate control and authority about the information that describes them.

The property model has dominated national discussions of privacy policy[11]; indeed, many of the live debates take a property model for granted. For example, whether a consumer's control is exercised by opting into a data collection program or by opting out of it assumes that the data is the consumer's to control. Thus, standard proposals for a federal omnibus privacy law fall somewhere along the spectrum of property rules, from a super-property style of right enshrined in EU law (where the GDPR gives people an inalienable right to control personal data by clawing it back for deletion, and by demanding services on the same terms as other consumers[12]) to a weak form of property that allows companies to collect data by default as long as consumers have an opportunity to opt out. Where the law falls on this spectrum is very consequential, but it is not the only way to approach privacy problems.

The alternative is a harm- or risk-based approach, which is the mode of regulation that guides most of tort law. And it is this harm-based approach that has guided the Federal Trade Commission in the last several years. Outside specific sectors like health[13] and credit reporting[14], privacy rights have been enforced by the FTC through its authority to guard against unfair and deceptive trade practices[15], but the unfairness and deception doctrines are guided by risks of substantial and concrete injuries rather than by user control.[16]

"Outside specific sectors like health and credit reporting , privacy rights have been enforced by the FTC through its authority to guard against unfair and deceptive trade practices , but the unfairness and deception doctrines are guided by risks of substantial and concrete injuries rather than by user control."

At first blush, this may sound like a bad deal for consumers because lack of user control could be seen as ipso facto injury. But risk-based regulations have some advantages. First, consumers can be protected from foreseeable risks *even if* they have opted in (or have not opted out) from a particular data transaction. At the same time,

---

[11] Among the laws using notice and consent as core mechanisms for protection: The European Data Protection Directive (which preceded the EU's General Data Protection Regulation), Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 13(2), 1995 O.J. (L 281) 31; The California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100, 1798.120.

[12] Art. 7 GDPR.

[13] The Health Information Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[14] The Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §1681

[15] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy,* 114 COL. L. REV. 583.

[16] *See* FTC Policy Statement on Deception (1983); FTC Policy Statement on Unfairnes (1980).

liability rules avoid the potential for overprotection when consumers distrust a new data practice that is actually socially and even personally beneficial. Indeed, the FTC, with its investigatory powers and team of economists, are in a much better position than individual consumers to evaluate whether a data-related bargain with a company is a good or bad deal for consumers. There is reason to think that people are hypervigilant and overly wary of new information technologies given that technology (along with immigration) causes a persistent, exaggerated, and well-documented sense of threat to humans.[17]

The Federal Trade Commission's harm-based approach to privacy regulation rests on a few practical and legal fundamentals. To the extent privacy rights are meant to entrench consumer expectations, the preservation of a status quo runs into the FTC's other mission to ensure market competition. The evolution of the FTC's unfairness and deception policies have also been informed by First Amendment case law like *Central Hudson v. Public Service Commission*[18], and more recent cases like *Sorrell v. IMS Health*[19] make a free speech analysis of any new privacy laws all the more imperative.[20] So even to the extent American privacy law is inadequate at the moment, it is important to remember that it has been shaped by a wealth of pragmatic and constitutional considerations.

WHAT DO WE KNOW ABOUT NOTICE & CONSENT?

Abundant evidence shows that privacy defaults are very sticky. Consumers rarely alter the defaults in privacy settings[21], and the drafting of privacy notices has almost no effect on behavior.[22] Even when consumers are paying attention to privacy options, they rarely forego a service or benefit that they would otherwise want in order to protect their privacy.[23] Outside Facebook, where sustained attention and criticism has caused a greater proportion of users to

---

[17] Bryan Caplan, THE MYTH OF THE RATIONAL VOTER 23-93 (2007).

[18] 447 U.S. 557 (1980) (applying intermediate scrutiny to non-deceptive commercial speech). *See also Trans Union v. Federal Trade Commission*, 81 F. 3d 228, 235 (1996) (suggesting that the FTC's interpretation of the Fair Credit Reporting Act as applied to targeted advertising could violate First Amendment intermediate scrutiny).

[19] 131 S.Ct. 2653 (2011)

[20] Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014).

[21] Adam S. Chilton & Omri Ben-Shahar, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. LEG. STUD. 41 (2016); Eric J. Johnson et all., *Defaults, Framing and Privacy: Why Opting In-Opting Out,* 13 MARKETING LETTERS 5 (2002).

[22] Lior J. Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEG. STUD. 569 (2016); Adam S. Chilton & Omri Ben-Shahar, *Simplification of Privacy Disclosures: An Experimental Test,* 45 J. LEG. STUD. 41 (2016). In my own work, I have found that privacy-related notices are often wasteful and do not change consumer choices. Dramatic just-in-time disclosures have the best potential to change behavior, but they also run the risk of exaggerating a sense of threat and distorting the consumer's evaluation of other criteria. Jane Bambauer et al., *A Bad Education,* 2017 IL. L. RE V. 109 (2017).

[23] Lior J. Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?,* 45 J. LEG. STUD. 569 (2016); Susan Athey et al., *The Digital Privacy Paradox: Small Money, Small Costs, Small Talk,* NBER WORKING PAPER NO. 23488 (2017); Alessandro Acquisti, *Privacy and Human Behavior in the Age of Information,* 347 SCIENCE 509 (2015) (providing a summary of related scholarship).

change their privacy settings[24], the great majority of consumers do not flip the default setting. This means that under a notice and choice regime, the practical result of an opt-in system is to severely restrict the service.

> *"On balance, consumers are not greatly interested in managing the particulars of their personal data."*

All of this suggests that on balance, consumers are not greatly interested in managing the particulars of their personal data.[25] This is not because they do not care, but because they are uncertain about the upsides and downsides of their bargains in the digital economy.

The GDPR and other opt-in regimes rest on an assumption that on balance, privacy is better for consumers than data use, but the empirical evidence does not bear this out. For example, one longstanding source of concern is the use of greater amounts of personal data for making lending decisions. A study of privacy defaults in the laws regulating home loans in the San Francisco Bay area found that loan applicants living in the counties that set privacy as the default paid higher interest rates and defaulted at greater rates than the counties that set data flow as the default, even after controlling for confounders, because banks could not match applicants to loans as well, so the costs of risk were, of course, passed along to the consumers.[26] And a study of online advertising in the EU before and after tailored advertising restrictions came into effect found that advertisements with disruptive noises and videos and websites with more specific (less general interest) content were the relative beneficiaries of the new restrictions.[27] More generally, with scrutiny, our collective instincts about Big Data tend to be inaccurate and pessimistic. For that reason, the government best serves consumers not by giving them more *control*, but by doing the substantive work of defining an informational harm that should be deterred.

WHAT HARMS ARE WE TRYING TO MITIGATE THROUGH PRIVACY LAW?

Once we dispense with the assumption that the goal of privacy is user control for its own sake, we are left with the harder questions: what are the societal risks that privacy law is meant to address?

---

[24] Andrew Perrin, *Americans Are Changing Their Relationship with Facebook,* PEW RESEARCH CENTER (2018), available at http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/.

[25] Tal Zarsky, *Privacy and Manipulation in the Digital Age,* 20 THEORETICAL INQUIRIES IN LAW 157, 162 (2019).

[26] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis,* 46 RAND J. OF ECON. 1 (2015). This is consistent with the more general phenomenon of risk-based lending markets. *See* Wendy Edelberg, *Risk-Based Pricing of Interest Rates for Consumer Loans,* 53 J. MONETARY ECON. 2283 (2006).

[27] Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising,* 57 MANAGEMENT SCIENCE 57 (2011).

Right now, public policy debates are focused on three privacy-related concerns: (1) Bias and discriminatory treatment in Big Data systems; (2) Consumer manipulation through behavioral targeting; and (3) Anticompetitive behavior by the large, established platforms (Google, Amazon, Facebook, and Apple.) Each of these societal risks deserves serious and sustained attention, and each may require regulatory intervention. But none are well-served by the California or European privacy laws.

1. *Big Data Bias*

Concern about Big Data processes effects on the distribution of resources or costs is one of the primary concerns for consumer advocates and regulators. Senator Cory Booker's question to the panel of experts who testified at the March hearing is a model. He asked:

How easy is it for seemingly non-sensitive information like a ZIP Code to become a proxy for protected class or other sensitive information? How can that information be used to discriminate?[28]

I appreciate this question because it gets at, and helps define, the societal harms that privacy laws are meant to prevent. One principal concern about the collection and sale of large amounts of personal data is that the data may be used in ways that perpetuate or exacerbate inequalities along race, gender, and class lines. Books like *Weapons of Math Destruction*[29] and academic articles such as *Big Data's Disparate Impact*[30] help explain how this can happen. But it is important to separate the theoretically possible from the pragmatically probable. Thoughtful uses of algorithms have the potential to reduce bias—indeed they have tremendous promise for optimizing decisions to comply with a particular notion of fairness far better than any human system could. But what "fairness" should mean is a distinctly human decision.

"Thoughtful uses of algorithms have the potential to reduce bias—indeed they have tremendous promise for optimizing decisions to comply with a particular notion of fairness far better than any human system could. But what "fairness" should mean is a distinctly human decision."

To illustrate, consider the much maligned[31] recidivism risk scores (such as the COMPAS scores) that are intended to measure the chance that a person in the criminal justice system will be arrested for another crime

---

[28] Jane Bambauer, RESPONSES TO WRITTEN QUESTIONS FROM THE SENATE JUDICIARY COMMITTEE: THE LIKELY IMPACT OF THE GDPR AND THE CCPA ON INNOVATION AND CONSUMER WELFARE (April 3, 2019), available at https://pep.gmu.edu/wp-content/uploads/sites/28/2019/04/J_Bambauer_Response_to_Written_Questions_April_3_2019.pdf.

[29] Cathy O'Neil, WEAPONS OF MATH DESTRUCTION (2016)

[30] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CAL. L. REV. 671 (2016).

[31] Julia Angwin et al., *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks,* PROPUBLICA (2016).

if released.[32] These scores could be biased by virtue of the chosen outcome variable—likelihood of arrest. There is good reason to believe that police are often more likely to detect and arrest Latinos and African-Americans than whites who commit the same crimes, in part because low income and minority neighborhoods are patrolled more often.[33] So even before predictors like zip code have the chance to create racial disparities, the choice of predicted outcome variable can cement inequities. (What we'd really like to predict is likelihood of *committing a crime*, but it is not surprising that arrests are used as the closest available alternative.)

If the chosen outcome is sufficiently neutral, an algorithm may still have a disparate impact on minorities even when race is not included as a predictor in the model. However, it is not obvious which disparate impacts should be actionable, particularly when the variables that correlate with race also correlate with a legitimate outcome that is being predicted. In human systems, experts often look for differences in the success or failure rates for members of different groups who are scored and treated the same way. (Becker 1957). For example, in Floyd v. NYPD, the case challenging the practices of the NYPD stop and frisk program, the fact that frisks of African-Americans were *less likely* to produce a weapon than frisks of whites showed that police were using a different standard for minorities. This problem, though, will usually not occur with machine learning algorithms because they work backwards from the predicted outcome. Every variable that is included in a machine learning model will be used in service of making the prediction score match the outcomes that are observed later.

However, there are other measures of fairness that can be considered, such as whether a member of a disadvantaged group is more likely to produce a false positive, or less likely to get the benefits of a false negative, than a member of the majority group. These different versions of "fairness" are in tension with one another, so making improvements for one can make others worse.

At some point, it may be necessary to have public commitments to a specific definition of discrimination and fairness in the digital era. That definition would have to work out compromises between competing interests in accuracy, equitable distribution of errors, and race-neutral treatment.[34] But it would be premature to do so now because the *human* decision-making

---

[32] These scoring systems do not use the vast amount of data and sophisticated processing that AI/machine learning is capable of, but they are valuable for showing that problems with bias are real, and also misunderstood.

[33] *See, e.g.,* Samuel Gross & Katherine Barnes, *Road Work: Racial Profiling and Drug Interdiction on the Highway,* 101 MICH. L. REV. 651 (2002).

[34] Jon Kleinberg, Jens Ludwig, Sendhil Mullainathan, and Cass Sunstein provide a good start. Jon Kleinberg et al., *Discrimination in the Age of Algorithms,* NBER WORKING PAPER NO. 25548 (2019) ("The existence of disparate impact is clear; the data will prove it, and also show its magnitude. We can also attempt to specify the practice that gives rise to those impacts. Then the question is the standard one: Can the disparate impact be justified, given the relevant standard? That is the same question that would be asked if an algorithm were not involved. The presence of the algorithm goes further – it makes it possible to quantify the tradeoffs that are relevant to determining whether there is 'business necessity' (or some other justification for disparate impact). Algorithms by construction produce not just a single ranking of applicants. They can produce a set of rankings that vary based on one's tolerance for disparate impact. For each of these rankings, they additionally quantify their effect on the objective, such as sales. This allows us to answer exactly the question, 'What is the magnitude of the disparate impact, and what would be the cost of eliminating or reducing it?'").

that digital tools augment or replace are at least as flawed along the same metrics (often more so, and with less transparency).[35] The few studies that compare the effects of using recidivism scores to bail and sentencing decisions made in their absence find that jailing is reduced for members of *every* race, and that pretrial detentions could be even further reduced if judges are removed from the decision-making.[36]

These findings are at odds with the way COMPAS scores are portrayed in the popular media, but they are consistent with studies in other areas finding that machine algorithms, as actually implemented, tend to improve race and gender disparities rather than exacerbate them. One study found that a hiring algorithm had a positive effect on the success rate of racial minority applicants compared to the status quo recruiting process[37], and another found that a machine learning algorithm could be used to select corporate directors who were more likely to be female *and* more likely to outperform the directors actually selected by the boards.[38] Home mortgages will tend to have lower interest rates and lower default rates when banks are able to make use of Big Data profiles that go beyond the income and credit score information that is typically collected, suggesting that machine learning has promise for helping low income applicants prove that they are more creditworthy than loan officers have historically thought.[39] And a study of risk scores used by child protective service centers found that when human decision-makers deviated from the recommendation of a scoring system, they tended to screen more black families into the high risk treatment (meaning that racial disparities would be less bad if the human decision-makers were bypassed altogether).[40]

So, it is very likely that some factors used by Big Data algorithms will correlate with race. But this is true of the factors used by human and "little data" decision-makers, too, and it does not mean on its own that something untoward or legally discriminatory has occurred. With guidance,

---

[35] Policy analysis should compare existing and future problems of AI to the counterfactual by asking what sort of distributional outcomes we could expect in the absence of the technology. *See* Bo Cowgill & Catherine Tucker, *Algorithmic Bias: A Counterfactual Perspective,* NSF WORKING PAPER: TRUSTWORTHY ALGORITHMS (2017).

[36] John Kleinberg et al., *Human Decisions and Machine Predictions,* NBER WORKING PAPER NO. 23180 (2017). *See also* Megan Stevenson, *Assessing Risk Assessment in Action,* 103 MINN. L. REV. 303 (2018) (finding that a law requiring judges to at least consider risk assessment scores caused a short-term reduction in pretrial detention, but that the reduction faded over time as judges returned to their previous habits. Stevenson also found that pretrial arrests increased when the scores were influencing judge's decisions, but pretrial arrests for violent crimes went down slightly. Stevenson did not find promising reductions in the race gap, though.)

[37] Bo Cowgill, *Productivity in Humans and Algorithms: Theory and Evidence from Resume Screening* (working paper).

[38] Isil Erel et al., *Selecting Directors Using Machine Learning,* NBER WORKING PAPER NO. 24435 (2018).

[39] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis,* 46 RAND J. OF ECON. 1 (2015). *See also* Will Dobie et al., *Measuring Bias in Consumer Lending*, NBER WORKING PAPER NO. 24953 (2018). By contrast, studies of human-driven mortgage lending decisions continue to find racial bias even after controlling for credit history and income. *Id.*

[40] Alesandra Chouldechova, *A case study of algorithm-assisted decision making in child maltreatment hotline screening decisions,* 81 PROC. MACHINE LEARNING RESEARCH 1 (2018) (citing Alan J. Dettlaff et al., *Disentangling Substantiation: The Influence of Race, Income, and Risk on the Substantiation Decision in Child Welfare,* 33 CHILDREN AND YOUTH SERVICES REVIEW 1630 (2011)).

antidiscrimination law can adapt so that notions of discriminatory treatment or disparate impact have even more coherence and clarity than they do today.

2. Consumer Manipulation

Consumer advocates and lawmakers are concerned that personal data can be used to target individuals with hyper-customized messaging (including advertising and political pleas) that activate the reader's short-term thinking or irrational decision-making, or that segments people into "filter bubbles" that reduce tolerance and cultural integrity.

"Oftentimes, privacy rules that restrict collection and access to personal data are mistaken as nearly costless solutions to the perceived threat of hyper-targeted content."

Oftentimes, privacy rules that restrict collection and access to personal data are mistaken as nearly costless solutions to the perceived threat of hyper-targeted content. For example, Senator Lindsey Graham asked a panel of technology experts how important tracking-based behavioral advertising was to the overall economic ecosystem and to a service provider's bottom line when he visited a website with golf-related content.[41] The panel of experts seemed to agree that contextual advertising based only on the content of the golf website would provide roughly the same revenue as behavioral advertising. One panelist mentioned, as further support, that the New York Times website saw increased profits from advertising after it decided to discontinue behavioral advertising on its website. The exchange would have led the unwary to believe that behavioral advertising could be killed off with little effect to the World Wide Web. This is not so. The aggregate amount spent on advertising is likely to be reduced somewhat when strong restrictions on data-collection are imposed. More importantly, the advertising dollars that *are* spent will be redistributed in ways that do not serve the public.

To see why, imagine you visit two websites: one for golf enthusiasts, and one with general interest news articles. With the aid of data aggregators and advertising exchanges, both websites will profit about equally from your visit because both could deliver advertising related to golf, or related to your location, or to your other interests and preferences. On the other hand, if tracking were prohibited either as a default or because you opted out, then the prospects of the two websites are very different. The advertising dollars will flock to the golf website and away from the general interest news website. Without behavioral advertising, websites will face market pressure to produce more content that allows advertisers to match themselves to end users through context.

The implications may not seem so troubling when comparing golf to general interest websites, but imagine how these changes would affect competing news websites, or content about health and medical information. The high value content that will attract advertisers are the stories that

---

[41] Senate Judiciary Committee Hearing, GDPR & CCPA: Opt-ins, Consumer Control, and the Impact on Competition and Innovation (March 12, 2019), video available at https://www.judiciary.senate.gov/meetings/gdpr-and-ccpa-opt-ins-consumer-control-and-the-impact-on-competition-and-innovation.

help fragment readers into market segments by signaling their ideology or other personal characteristics based on content.

My concerns here are not theoretical; a study of the effects of the EU Data Protection Directive (the privacy framework that was in place in Europe before the GDPR took effect) found that the efficacy of advertising in Europe was reduced, but the reductions were not uniform.[42] "Websites that had general content unrelated to specific product categories (such as news and media services) experienced larger decreases in ad effectiveness after the laws passed than websites that had more specific content (such as travel or parenting websites). Customers at travel and parenting websites have already identified themselves as being in a particular target market, so it is less important for those websites to use data on previous browsing behavior to target their ads."[43]

Moreover, some of the panelists suggested that advertising revenues for a website are not highly dependent on behavioral advertising. This is not accurate. Behavioral advertising has a "click-through" rate 670% higher than contextual advertising[44]. Some of this difference in click-through is the result of behavioral targeting identifying consumers who would buy the product or service anyway, irrespective of whether an ad were ever served to them, so the simple figures comparing behavioral targeting click-through rates and other forms of advertising can exaggerate the differences.[45] Nevertheless, today, an ad placed with the help of behavioral data will pay the website much more than an ad placed without data (on average). The fact that the New York Times' revenues have continued to rise since ending behaviorally targeted ads in Europe may be explained by the steady increase in its readership and subscriber base since the election of President Trump; the *Times* had just over one million subscribers before the 2016 election and now has over four million.[46] Changing the privacy rules will change content and services in some ways that consumers will not favor. And since the effects are difficult to predict, it makes all the more sense for the government to clearly define illegal manipulation and prohibit those data uses rather than giving consumers the opportunity, but also the task, of figuring out for themselves what types of data practices are harmful.

---

[42] Avi Goldfarb & Catherine E. Tucker, *Privacy, Regulation, and Online Advertising,* 57 MANAGEMENT SCIENCE 57 (2011).

[43] *Id*. *See also* Catherine E. Tucker, *The Economics of Advertising and Privacy* ("The reduction we measured is particularly pronounced for websites offering content that is not easy to match to advertising (such as news websites and media services). It is also more pronounced for non-intrusive and smaller ads, since their appeal rests primarily on the presentation of informative rather than attention-grabbing messages. This suggests that privacy regulation might change the web landscape in unanticipated ways, with advertising becoming even more intrusive, and marketers shifting their media buys away from sites such as news providers that are difficult to match with relevant advertising.")

[44] Jun Yan et al., *How Much Can Behavioral Targeting Help Online Advertising?,* PROC. OF THE 18TH INT. CONF. ON WORLD WIDE WEB 261 (2009).

[45] Brett R. Gordon et al., *A Comparison of Approaches to Advertising Measurement: Evidence from Big Field Experiments at Facebook,* 38 MARKETING SCIENCE 193 (2019).

[46] Jaclyn Peiser, *New York Times Tops 4 Million Mark in Total Subscribers,* N.Y. TIMES (November 1, 2018); Rani Molla, *The 'Trump Bump' in the New York Times' Digital Subscription Growth Is Over,* RECODE (August 9, 2018). Another possibility is that the reporting in the *Times* may have changed since the election of Donald Trump as well such that the context of the articles are more ideologically skewed, and therefore send a signal for market segmentation.

Online tracking and data aggregators are popularly understood to reduce the power of consumers, but there is another way to see it. When ad networks can access data from aggregators and target ad dollars more effectively, it allows the consumers rather than the content-providers to control where the money goes. Each of us will reward whichever websites we like to visit, even if they don't cater to a well-defined market segment. Consumers who wish to opt out of tracking rarely understand that they are rewarding content providers who produce inherently commercial or highly segmented content. The winners in this system include Facebook and Google, because these companies can match ads to users without any help from third party data aggregators.[47] This leads to the third concern: the anticompetitive effects of tough privacy laws.

3. Market Power

Many lawmakers are concerned that large digital companies (like Amazon) have behaved in anticompetitive ways to achieve their market dominance[48], and require regulatory interventions of various sorts (including privacy laws) to protect consumers who are effectively forced to interact with them. The premise of this concern is likely wrong; the large digital firms are competitive and highly responsive to consumer preferences. But even if the market for digital services *were* distorted in a way that favors the large firms, omnibus privacy laws can make that distortion worse.

The California Consumer Privacy Act is designed to solve the problem of limited consumer choice by forcing firms not only to allow consumers to opt out of data collection and use, but also to treat those consumers who do opt out the same way as other customers. (This requirement appears in the "non-discrimination" provision of the Act.) This provision is popular among advocates who lament the "take-it-or-leave-it" options that are currently offered to users, but the effect of the law is to force people who do not opt-out to subsidize the costs of the people who do.

To understand why I recommend a legal framework that permits a "take it or leave it" response, consider a website that earns its revenues from behaviorally targeted advertising. We know that an ad placed with the help of behavioral data will pay the website much more than an ad placed without data (on average).[49] Now, suppose that 25% of the website's visitors exercise their rights

---

[47] Indeed, the privacy rules promulgated by the FCC in 2016, but which never went into effect, were likely to *increase* the dominance of Facebook and Google by preventing internet service provider companies like Verizon from entering the market for data tailoring. *See* Howard Homonoff, *Facebook and Google Win From New FCC Privacy Regulations, And Everyone Else Loses,* FORBES.COM (October 31, 2016); Roger Entner, *FCC Should Whack Privacy Rules that Favor Google and Facebook,* THE HILL (February 15, 2017).

[48] For a description and critique of these arguments, *see* Seth B. Sacher & John M. Yun, *Twelve Fallacies of the 'Neo-Antitrust' Movement,* available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3369013.

[49] The fact that the New York Times' revenues have continued to rise since ending behaviorally targeted ads in Europe may be explained by the steady increase in its readership and subscriber base since the election of President Trump. Jaclyn Peiser, *New York Times Tops 4 Million Mark in Total Subscribers,* N.Y. TIMES (November 1, 2018).

under the CCPA to opt out of the data exchanges that permit behavioral ad targeting. What can the website do in response?

Suppose compliance with the CCPA antidiscrimination provision requires the website to treat everyone the same. Given the lost advertising revenue, the website may have to reduce the quantity or quality of their content, or increase the number of ads each viewer has to see. Either way, consumers who have not exercised their privacy rights will be forced to subsidize the services of those who have.

Alternatively, suppose the antidiscrimination provision allows the website to provide different services based on the different revenues they can expect to draw for the two types of consumers. In this case, the website could display more ads, untargeted as they must be, to the consumers who exercised their privacy rights. Or they could limit these consumers' access to content that had higher production costs. If this is permitted, the law would no longer force cross-subsidization, but it would also largely render the antidiscrimination provision moot.

These issues will become more complex with AI and machine learning services. Consider, for example, emerging health technologies. Advances in Machine Learning are already changing the practice of medicine because new programs can digest and learn from vast amounts of data about other patients to make customized recommendations. These programs can also update the therapeutic recommendations in real time as it receives and learns from the health outcomes data of its users.[50] Other applications can help hospitals predict how much staffing they will need based on non-health data that might have clues about an influx of new patients. But some of the most promising applications would have to merge data from disparate sources both within and outside the health sector, and the incentives to do this are likely to depend on being able to collect, purchase, and reuse personal data.[51]

The consent and control concepts in the CCPA cannot easily be applied to these developments. What would it mean for a patient to demand data deletion, or to opt out of sale? And in what way would the program have to avoid "discriminating" against a person who exercises these rights? Would the program have to be designed to work as well as possible while removing the data from the user? Would the company have to remove that user's data from the pooled dataset used to optimize the program's recommendations to all of its users, or could it safely rely on the exemption for deidentified data? Is it sensible or fair to allow a user to benefit from the past data shared by other patients without contributing his or her own data to the system? If the company declines service or offers inferior services to a user who exercises the deletion or opt-out right, it must be prepared to show that the differential treatment is "reasonably related to the value

[50] *See, e.g.,* the discussion of Ginger.io in Basel Kayyali et al., *The Big-Data Revolution in US Health Care: Accelerating Value and Innovation,* MCKINSEY REPORT (2013).

[51] Sonja Marjanovic et al., *Understanding Value in Health Data Ecosystems,* RAND RESEARCH REPORT (2017).

provided to the consumer by the consumer's data"[52]—a vague standard that is sure to deter experimentation.

The CCPA has the goal of siloing and minimizing personal data at a time when lawmakers should be facilitating more responsible and socially beneficial data-sharing. It is already very difficult to link databases and make them usable for a variety of purposes, and in the context of health the problem has profound consequences. For example, in the wake of the removal of the drug Vioxx from the market, Richard Platt, a professor at Harvard Medical School, showed that the fatal side effects of the drug could have been detected in just three months, rather than the five years it actually took, if health data across the country had been merged.[53] Large datasets of merged records will be vital for the success of some of the future Machine Learning applications, too. Since individual hospitals, clinics, and insurers have little incentive to give away their data, money (from sales to data aggregators) is a badly-needed lubricant.

"Another reason to pause before implementing significant privacy restrictions is that the regulations are likely to give the dominant firms an even **stronger** *market advantage."*

The same issues arise outside the healthcare context, albeit with different (often lower) stakes. With better information, loans and auto insurance plans can be better matched and managed, reducing prices, defaults, and accidents.[54]

Another reason to pause before implementing significant privacy restrictions is that the regulations are likely to give the dominant firms an even *stronger* market advantage. The potential conflict between consumer privacy and market competition is reflected in a question that Senator Chuck Grassley posed:

> ***Often times, comprehensive regulations end up just benefiting the large, entrenched entities that have teams of lawyers to ensure compliance. Should small businesses be treated differently in any federal data privacy framework? And if so, how?***

The theoretical and empirical literature indeed suggests that data privacy laws have adverse effects on smaller and newer firms.[55] For example, GDPR had a depressant effect on the ability

---

[52] This is particularly difficult language to interpret because the value of a consumer's data must be "provided to the consumer." It is not clear how direct the return of value to consumers must be.

[53] Barbara J. Evans, *Seven Pillars of a New Evidentiary Paradigm: The Food, Drug, and Cosmetic Act Enters the Genomic Era,* 85 NOTRE DAME L. REV. 419, 455-456 (2010).

[54] Jin-Hyuk Kim & Liad Wagman, *Screening Incentives and Privacy Protection in Financial Markets: A Theoretical and Empirical Analysis,* 46 RAND J. OF ECON. 1 (2015) (home loans); Prof. Omri Ben Shahar, Testimony at the Federal Trade Commission Informational Injury Workshop, 168-69 (December 12, 2017) (discussing the benefits of privacy-invasive auto insurance plans).

[55] James Campbell et al., *Privacy Regulation and Market Structure* 24 J. ECON. & MGMT. STRATEGY 47 (2015); Jian Jia et al., *supra* note 2.

of all European firms to attract venture capital, but new firms (within the first three years of operation) were much harder hit than the others.[56]

An approach to privacy that centers around harmful uses of data rather than user control will be less burdensome for all businesses (including startups) because they will not have to respond to individual consumers' requests, so long as their business model is a fair one that offers mutually beneficial services to its customers. The Federal Trade Commission, with its twin missions of enforcing consumer protection and antitrust laws, is uniquely well-positioned to understand the extent to which a privacy rule will exacerbate competition problems, and vice versa. For this reason, it would make sense to keep enforcement authority at the FTC with guideposts that direct the agency's work and bound its discretion.

STRENTHENING AND IMPROVING THE AMERICAN APPROACH TO PRIVACY REGULATION

A GDPR-style of privacy right that gives consumers and end users full control over personal information has enormous popular appeal, but despite the political demand, property-style privacy rights do not actually serve American consumer interests. They will burden the digital economy with transaction costs, and there is little reason to think that the compliance costs or behavioral changes will have a meaningful relationship to harm.

> *"An optimal privacy law will protect consumers from data-related harm while also protecting them from the less obvious costs of data siloing and underutilization."*

An optimal privacy law will protect consumers from data-related harm while also protecting them from the less obvious costs of data siloing and underutilization. It would preserve much of the underappreciated expertise that the Federal Trade Commission has developed to foster consumer protection and market competition over the last several decades. It would, in other words, hold firms responsible for breaches of care that place unjustified risks and costs on consumers without unduly focusing on consumer control.

Federal law should facilitate a means to identify and incisively reduce specific data uses and practices that are likely to cause harm to consumers. This approach is orthogonal to the California Consumer Privacy Act because it does not center around user consent. Consent rules expect each individual consumer to develop expertise on the data practices of the moment and guard their interests themselves.

There is some risk that consumers will fail to guard their interests when risk arises. The greater concern, though, is that consumers and companies will be reluctant to permit data to be gathered

[56] Jian Jia et al., *supra* note 2.

or sold or reused in novel ways, impoverishing the advances we've already seen and will continue to see in the digital economy.

A privacy statute will be more likely to endure through the age of AI and whatever comes next if it codifies and strengthens the work that the Federal Trade Commission has already done to broker compromises between consumer privacy and data-driven services. President Obama's draft 2015 Consumer Privacy Bill of Rights[57] and Senator Schatz's proposed Data Care Act[58] influenced my thinking about the key features of a responsible privacy law that can respond to concerns about the unsupervised expansion of personal data collection without promising an unworkable or ultimately harmful degree of user control.[59] The complex problems of modern personal data use are best managed through laws that recognize the following:

• Duty of Care to avoid unjustified consumer risk or injury

> *This duty includes, but is not limited to, a requirement to provide notice and consent if the firm will engage in unexpected and material data practices. The failure to provide effective notice for a data practice that would have caused consumers to behave differently or choose a different option (including possibly foregoing a product or service) would meet the materiality requirement.*

• Duty of Protection to secure personal data from unauthorized access.

> *This duty creates a uniform standard for data security based on industry best practices and clarifies the conditions under which a firm would have to notify consumers about a data breach.*

• Duty of Confidentiality limiting the disclosure of personal data to other firms and individuals who are bound by the same duties of care and protection.

> *This duty includes a requirement to reasonably ensure that a recipient of personal data is providing the same level of care and protection by vetting and, if appropriate, auditing the recipient. A company that has reason to know that its partner has violated a duty of care or protection must notify the FTC.*

• Federal Trade Commission rulemaking authority to define duties and responsibilities related to personal data practices

> *The FTC will be authorized, and even required in some cases, to generate and harness expertise and promulgate clear rules of the road for companies that use personal data.*

• Preemption of state law to provide predictable and uniform national coverage

---

[57] Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015.

[58] S.3744- Data Care Act of 2018.

[59] I am also grateful for comments and collaboration from Berin Szoka, Geoff Manne, and Gus Hurwitz, who reviewed and helped revise the draft language presented here.

This Bill would preempt the California Consumer Protection Act, but would require all U.S. companies to comply with obligations that overlap with the CCPA to some degree.

• Shared enforcement authority between the Federal Trade Commission and state attorneys general

The FTC and State AG offices will share the authority to seek declaratory or injunctive relief and, in cases where a firm had actual knowledge, significant monetary fines for violations of the duties

The draft bill, attached as an appendix to this report, provides a model that incorporates all of these ideas.

APPENDIX

116TH CONGRESS

2D SESSION

H.R./S. ____

To establish duties for consumer service providers that protect consumer interests in privacy, security, innovation, and free speech.

IN THE _____ OF THE UNITED STATES

A BILL

To establish duties for service providers with respect to consumer data, and to provide national uniformity of regulation.

SECTION 1. SHORT TITLE.

This Act may be cited as the ‘‘Data Stewardship Act of 2019’’.

SEC. 2. DEFINITIONS.

In this Act—

(1) the term ‘‘Commission’’ means the Federal

Trade Commission;

(2) the term “business” means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity engaged in interstate commerce, and that has annual receipts in excess of the U.S. Small Business Administration size standard for the business’ industry, as calculated by the U.S. Small Business Association

(3) the term ‘‘consumer’’ means a natural person, in his or her personal capacity (but not in his or her capacity as an employee), in the United States whose personal information is collected, used, or shared by such business.

(4) the term ‘‘personal information” means any data that describes the characteristics or behavior of a consumer and that identifies the consumer by last name, social security number, phone number, physical address, or unique device

(5) the term “deidentified information” means data that describes the characteristics or behavior of a consumer and that does not identify the consumer by last name, phone number, physical address, or unique device, AND for which a business publicly commits to refrain from attempting to identify with an individual or device and adopts relevant controls to prevent such identification, AND

(A) makes any other alterations necessary to ensure that the data could not be linked as a practical matter to a specific individual or device; OR

(B) causes to be covered by a contractual or other legally enforceable prohibition on each individual or entity to which the business discloses the data from attempting to link the data

to a specific individual or device, and requires the same of all onward disclosures;

(6) the term ‘‘sensitive data’’ means any personal information that includes—

(B) personal information as defined in section 1302 of the Children’s Online Privacy Protection Act of 1998 (15 U.S.C. §6501) collected from a child (as defined in such section 1302);

(C) a Social Security number, driver’s license number, passport number, military identification number, or any other similar number issued on a government document used to verify identity;

(D) a financial account number, credit or debit card number, or any required security code, access code, or password that is necessary to permit access to a financial account of an individual;

(E) unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation that is used as an access code for authorized access to personal accounts;

(F) information sufficient to access an account of an individual, such as user name and password or email address and password;

(G) information that relates to the past, present, or future medical diagnosis of the individual; or

(H) the nonpublic communications or other nonpublic user-created content of an individual.

SEC. 3. PROVIDER DUTIES.

(a) IN GENERAL.—A business shall fulfill the duties of protection, care, and confidentiality under paragraphs (1), (2), and (3), respectively, of subsection (b).

(b) DUTIES.—

(1) DUTY OF PROTECTION.—A business shall—

(A) use relevant industry best practices to reasonably secure personal information from unauthorized access; and

(B) promptly inform a consumer about the nature and extent of any unauthorized access of sensitive data of that consumer.

(2) DUTY OF CARE.—A business may not use personal information, or data derived from personal data, in any way that:

(A) will result in a foreseeable and unjustified consumer injury that is substantial, not reasonably avoidable by consumers themselves, and not outweighed by countervailing benefits to consumers; OR

(B) will result in reasonably foreseeable and material harm to consumers' interests. A material harm is one for which a business has not provided effective notice, and for which a majority of consumers, or, if the product or service affects or is directed primarily to a particular group, a majority of that group, if fully apprised of the consequences of their transaction(s) with the business, would have chosen another option available to them at the time of their transaction(s) in lieu of the transaction(s) that took place.

(3) DUTY OF CONFIDENTIALITY.—A business—

(A) may not disclose or sell personal information to, or share personal information with, any other person except as consistent with the duties of protection and care under paragraphs (1) and (2), respectively;

(B) may not disclose or sell personal information to, or share personal information with, any other person unless that person enters into a contract with the business that imposes on the person the same duties of protection, care, and confidentiality toward the applicable consumer as are imposed on the business under this sub-section;

(C) shall take reasonable steps to ensure that the practices of any person to whom the business discloses or sells, or with whom the business shares, personal information fulfill the duties of protection, care, and confidentiality assumed by the person under the contract described in subparagraph (B). Such reasonable steps may include auditing, on a regular basis, the data security and data information practices of any such person receiving sensitive data; and

(D) shall promptly notify the Commission of any known or suspected breach of a duty of protection, care, or confidentiality by a contracting person through procedures designed by the Commission consistent with this Act.

(c) EXCEPTIONS.—

(1) REGULATORY SAFE HARBORS.—The Commission may promulgate regulations under section 553 of title 5, United States Code, to exempt categories of businesses from the requirement under sub-sections (a) and (b) based on specific circumstances or practices. The Commission may also

promulgate regulations under section 553 of title 5, United States Code, that create safe harbors such that a business complying with the promulgated regulations will automatically satisfy the requirements under sub-sections (a) and (b). In promulgating these regulations, the Commission shall consider, among other factors—the costs and benefits to consumers and to market competition if the requirement under subsection (b) are applied to the specific circumstances or practices under consideration. Any business complying with the terms of a regulatory safe harbor shall not be subject to enforcement actions under this Act.

(2) COMISSION-APPROVED CODES OF CONDUCT.— A business shall have a complete defense to any enforcement action based on a violation of this Act if it demonstrates with respect to such an alleged violation that it has maintained a public commitment to adhere to a Commission-approved code of conduct that covers the practices that underlie the suit or action and is in compliance with such code of conduct.

(3) DEIDENTIFIED DATA.—Deidentified information is not personal information under this Act.

(4) DISCLOSURES TO LAW ENFORCEMENT.— This Act does not restrict a business from disclosing personal information to federal, state, or local law enforcement agencies

(A) pursuant to a subpoena, court order, warrant, or similar legal process which appears lawful on its face;

(B) if the business is under a legal obligation to report suspected criminal activity; or

(C) if the business has knowledge or a good faith belief that criminal activity may have occurred.

(5) DELETED DATA.— The term "personal information" shall not include data that a business deletes.

(6) EMPLOYEE INFORMATION.— The term "personal information" shall not include an employee's name, title, business address, business email address, business telephone number, business fax number, or any public licenses or records associated with the employment, when such information is collected or used by the employee's employer or another business, in connection with such employment status.

(7) CYBERSECURITY DATA.— The term "personal information" shall not include cyber threat indicators collected, processed, created, used, retained, or disclosed in order to investigate, mitigate, or otherwise respond to a cybersecurity threat or incident, when processed for those purposes.

SEC. 4. ENFORCEMENT.

(a) ENFORCEMENT BY COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 3 by a business shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. §57a(a)(1)(B)). Conversely, a practice of a business covered by this act that relates solely to the collection, retention, use, or dissemination of personal information shall not be considered an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act unless the practice violates section 3 of this Act.

(2) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. §§41 et seq.) were incorporated into and made a part of this Act.) Any person who violates section 3 shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. §41 et seq.).

(B) REMEDIES.—The Commission is empowered to enforce the provisions of this Act through actions for declaratory and injunctive relief following the procedures provided in 15 U.S.C. § 45. The Commission may also seek restitution to consumers of any money paid by consumers who were harmed by a violation of this Act, or disgorgement of profits made by businesses as a result of such a violation. Except as provided in subparagraph (C), the Commission shall not seek civil penalties.

(C) CIVIL PENALTIES.—A business that is found, in an action brought under paragraph (1), to have knowingly violated section 3 with a bad faith intent to defraud or seek unconscionable advantage shall, in addition to any other remedy otherwise applicable to a violation of section 3, be liable for a civil penalty equal to the amount calculated by multiplying—

(A) the greater of—

(i) the number of days during which the business

was not in compliance with that section; or

(ii) the number of end users who were harmed as a result of the violation, by

(B) an amount not to exceed the maximum civil penalty for which a person, partnership, or corporation may be liable under section 5(m)(1)(A) of the Federal Trade Commission Act (15 U.S.C. §45(m)(1)(A)).

(3) RULEMAKING AUTHORITY AND MANDATES.—The Commission shall promulgate regulations under this Act in accordance with 5 U.S.C. §553. Enforcement under this section may not commence based on a violation of this Act unless and until the Commission has promulgated regulations clarifying the standard for the duty alleged to have been breached.

(b) ENFORCEMENT BY STATES.—

(1) AUTHORIZATION.—Subject to paragraph (3), in any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is threatened or adversely affected by a practice of a business that violates section 3, the attorney general of the State may, as parens patriae, bring a civil action against the business on behalf of the residents of the State in an appropriate district court of the United States to obtain declaratory or injunctive relief, or to obtain civil penalties consistent with paragraph (2).

(2) CIVIL PENALTIES.—A business that is found, in an action brought under paragraph (1), to have knowingly violated section 3 with a bad faith intent to defraud or seek unconscionable advantage shall, in

addition to any other remedy otherwise applicable to a violation of section 3, be liable for a civil penalty equal to the amount calculated by multiplying—

(A) the greater of—

(i) the number of days during which the business was not in compliance with that section; or

(ii) the number of end users who were harmed as a result of the violation, by

(B) an amount not to exceed the maximum civil penalty for which a person, partnership, or corporation may be liable under section 5(m)(1)(A) of the Federal Trade Commission Act (15 U.S.C. §45(m)(1)(A)).

(3) PRIVILEGES OF FEDERAL TRADE COMMISSION.—

(A) NOTICE TO FEDERAL TRADE COMMISSION.—

(i) IN GENERAL.—Except as provided in clause (iii), the attorney general of a State shall notify the Commission in writing that the attorney general intends to bring a civil action under paragraph (1) before initiating the civil action.

(ii) CONTENTS.—The notification required under clause (i) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(iii) EXCEPTION.—If it is not feasible for the attorney general of a State to provide the notification required under clause (i) before initiating a civil action under paragraph (1) without risking irreparable

harm, the attorney general shall notify the Commission immediately upon instituting the civil action.

(B) INTERVENTION BY FEDERAL TRADE COMMISSION.—The Commission may—

(i) intervene in any civil action brought by the attorney general of a State under paragraph (1); and

(ii) upon intervening—

(I) be heard on all matters arising in the civil action; and

(II) file petitions for appeal of a decision in the civil action.

(4) INVESTIGATORY POWERS.—Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary or other evidence.

(5) PREEMPTIVE ACTION BY FEDERAL TRADE COMMISSION.—If the Commission institutes a civil action or an administrative action with respect to a violation of section 3, the attorney general of a State may not, during the pendency of the action, bring a civil action under paragraph (1) against any defendant named in the complaint of the Commission based on the same set of facts giving rise to the alleged violation with respect to which the Commission instituted the action.

(6) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in—

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(7) ACTIONS BY OTHER STATE OFFICIALS.—

(A) IN GENERAL.—In addition to civil actions brought by attorneys general under paragraph (1), any other consumer protection officer of a State who is authorized by the State to do so may bring a civil action under paragraph (1), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(B) SAVINGS PROVISION.—Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

SEC. 5. NONENFORCEABILITY OF CERTAIN PROVISIONS WAIVING RIGHTS AND REMEDIES.

The rights and remedies provided under this Act may not be waived or limited by contract.

SEC. 6. RELATION TO LAWS.

(a) PREEMPTION OF STATE LAW—The provisions of this Act shall supersede any provisions of the statutes, laws, regulations, rules, ordinances, requirements, or the equivalent, of any State, or any locality or political subdivision of a State, including but not limited to, any tort, duty, or consumer protection or unfair practice law, to the extent that such provisions serve as the basis for enforcement as it relates to the privacy or security of personal information. No State, or any locality or political subdivision of a State, shall adopt, maintain, enforce, impose, or continue in effect any such provision after the effective date of this Act.

(b) OTHER FEDERAL LAWS.

(1) IN GENERAL—Except as otherwise provided in paragraph (2) this Act shall supersede any other Federal statute or regulation relating to the privacy or security of personal information.

(2) This Act shall not be construed as superseding any of the following laws:

(A) The Children's Online Privacy Protection Act (15 U.S.C. §§6501 et seq.);

(B) The Communications Assistance of Law Enforcement Act (47 U.S.C. §1001 et seq.);

(C) Section 227 of the Communications Act of 1934 (47 U.S.C. §227);

(D) The Fair Credit Reporting Act (15 U.S.C. §1681 et seq.);

(E)The Health Insurance Portability and Accountability Act (Public Law 104-191);

(F) The Electronic Communications Privacy Act;

(G)The Driver Privacy Protection Act (15 U.S.C. §§2721 et seq);

(H) The Federal Aviation Act, as amended (49 U.S.C. §§40101 et seq.); and

(I) Section 230 of the Communications Decency Act (47 U.S.C. §230)

SEC. 7. EFFECTIVE DATE.

(a) IN GENERAL.—This Act shall take effect on the date of enactment of this Act.