THE UNIVERSITY OF ARIZONA
James E. Rogers
College of Law

The Perils of Privacy as Property:
The Likely Impact of the GDPR and the CCPA on Innovation and Consumer Welfare

March 12, 2019
Testimony before the Senate Judiciary Committee

Jane Bambauer
Professor of Law, University of Arizona
Director, Program on Economics & Privacy at George Mason University Antonin Scalia Law School

Chair Graham, Ranking Member Feinstein, and Members of the Committee, it is an honor to be able to speak with you about the design of the GDPR and the CCPA, and the impact that they are likely to have on consumer welfare and technological innovation. I have devoted my career to privacy and information law because poorly constructed privacy laws can frustrate the interests of the very people they are meant to protect.

I am delighted that Congress is focused on crafting a strong and uniform federal privacy statute. My goal is to share some of what I know from my own research and from the law and economics literature about the possible pitfalls as you move forward.

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 that there has been a significant reduction in the quantity and size of venture capital investments across all sectors in Europe, causing millions of dollars per week in opportunity costs.[1] Start-ups and young firms lose out more often than established firms.[2] 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 firms.[3] 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.

The CCPA is likely to cause similar effects. It is, in essence, a light version of the GDPR. Thus, we can expect a difficult transition period once the law comes into effect because the legislation introduces new, vague concepts such as the anti-discrimination provisions.[4] And even after a painful transition phase, the law will cause long-term drag on innovation.

This should give us 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.[5] And contrary to popular perception, there is more competition and

[1] Jian Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment,* NBER WORKING PAPER NO. 25248 (2018).
[2] *Id.*
[3] 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).
[4] The California Consumer Privacy Act, Cal. Civ. Code §1798.125.
[5] 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.

less concentration in the tech sector than there was in the manufacturing sector during its heyday.[6]

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 identify and permit innovations that may on the surface seem creepy. Because the Federal Trade Commission has developed this expertise, Congress should facilitate their work responding to concrete risks and harms.

Two Views of Privacy: Property Rules and Liability Rules[7]

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.[8] The core value of the FIPPs is a property-style right vested in the 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[9]; 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[10]) 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.

---

[6] 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 middle of the income distribution will reverse when we are further along in the transition to an AI-supported economy.)

[7] 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).

[8] U.S. DEPT. OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973).

[9] 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.

[10] Art. 7 GDPR.

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[11] and credit reporting[12], privacy rights have been enforced by the FTC through its authority to guard against unfair and deceptive trade practices[13], but the unfairness and deception doctrines are guided by risks of substantial and concrete injuries rather than by user control.[14]

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, 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.[15]

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*[16], and more recent cases like *Sorrell v. IMS Health*[17] make a free speech analysis of any new privacy laws all the more imperative.[18] 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?

---

[11] 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.).

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

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

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

[15] BRYAN CAPLAN, THE MYTH OF THE RATIONAL VOTER 23-93 (2007).

[16] 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).

[17] **131 S.Ct. 2653 (2011)**

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

Abundant evidence shows that privacy defaults are very sticky. Consumers rarely alter the defaults in privacy settings[19], and the drafting of privacy notices has almost no effect on behavior.[20] 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.[21] [22] Outside Facebook, where sustained attention and criticism has caused a greater proportion of users to change their privacy settings[23], 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.

All of this suggests that on balance, consumers are not greatly interested in managing the particulars of their personal data.[24] 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.[25] 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

[19] 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).

[20] 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).

[21] 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).

[22] *Id.*; Alessandro Acquisti, *Privacy and Human Behavior in the Age of Information,* 347 SCIENCE 509 (2015) (providing a summary of related scholarship).

[23] 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/.

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

[25] 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).

new restrictions.[26] More generally, with scrutiny, our collective instincts about Big Data tend to be inaccurate and pessimistic.

Strengthening 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. 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.

For the sake of discussion and idea generation, I have included with my written testimony a draft bill that codifies much of the regulatory work that the Federal Trade Commission has already done in this area, and expands the FTC's charge to incorporate some of the ideas found in President Obama's draft 2015 Consumer Privacy Bill of Rights[27] and Senator Schatz's proposed Data Care Act[28]. This draft bill is intended to respond to concerns about the unsupervised expansion of personal data collection and use without promising an unworkable or ultimately harmful degree of user control. Here are the key features that help it respond to the complex problems of data use:

- 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.

[26] Avi Goldfarb & Catherine E. Tucker, *Privacy Regulation and Online Advertising,* 57 MANAGEMENT SCIENCE 57 (2011).
[27] Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015.
[28] S.3744- Data Care Act of 2018.

• 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

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

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—

(i) 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 care and loyalty 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 or if the business has 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 harmed by 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.