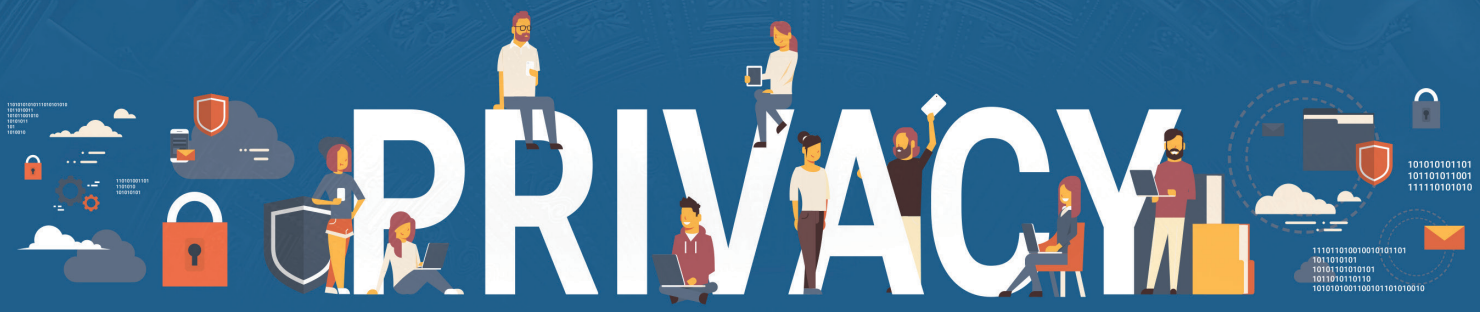
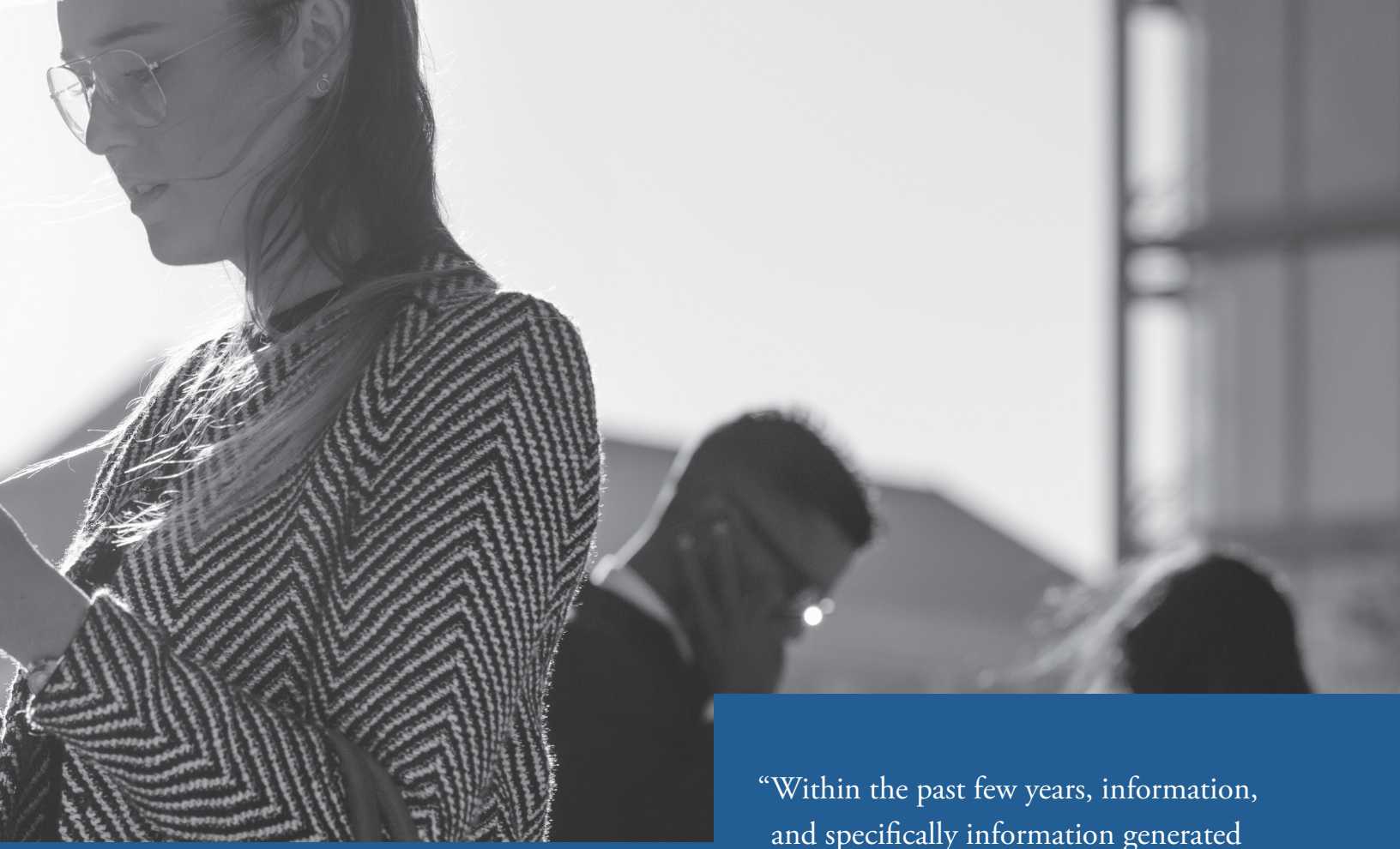
A FRAMEWORK FOR PRIVACY LEGISLATION



ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM



"Within the past few years, information, and specifically information generated by or about individuals, has become a key driver for the American economy. Companies from technology giants like Google and Facebook to main street stores have figured out how to monetize information about individuals."

Introduction

Privacy is *en vogue*. Policymakers from Washington, D.C. to Washington State are talking about it. They are holding meetings and proposing comprehensive legislation designed to control corporate access to, and use of, people's personal information.

Rather than solve a "privacy problem," many of the proposed and enacted legislation focuses on corporate behavior—what corporations must do to collect and use data. While most state proposals make it more difficult to collect and use information, the laws do not operate as complete bars to the use and collection of data. The type of regulations proposed by some states will do little other than restrict the flow of information, constrict the online marketplace, and ensconce incumbent platforms.

Most states, and the federal government, already have a model for dealing with any privacy problem. The Federal Trade Commission and state consumer protection regimes are already well-equipped to protect consumers when a company fails properly to secure a person's data, when it violates its promises to consumers, or when it engages in conduct that harms consumers such as failing to fulfill its terms of service.

There is a need for a measured, informed discussion about the roll information plays in people's lives.[1] Within the past few years, information, and specifically information generated by or about individuals, has become a key driver for the American economy. Companies from technology giants like Google and Facebook to main street stores have figured out how to monetize information about individuals.

Platforms offer services or products people deem valuable. People are willing to exchange information in return for access to mobile phone app GPS services, email, social media, and so much more. People are willing to generate information and share that information on social media platforms. People willingly stream their video game performances, create various types of videos, post their political opinions online, or share cute kitten videos.

Despite the benefits innovators are providing, policymakers are debating how the government should regulate the flow of information. Some policymakers and activists are calling for greater regulations, restricting what companies may do with information, how they may acquire information, and how they may interact with consumers. The calls for regulation seem bipartisan, with the political right and left both agreeing the government needs to regulate "big tech" and its access to information. Policymakers tend to justify regulatory proposals under the guise of "consumer protection." Yet, current proposals or existing "privacy" laws focus on corporate behavior rather than answering one essential question: What consumer harms are policymakers trying to prevent or protect against?[2]

Policymakers should endeavor to protect consumers from actual, concrete harm while allowing the greatest flexibility for innovators and the private sector. Existing consumer protection standards provides flexibility, while providing innovators the space they need to create new products. This is not to say that enforcement mechanisms are currently perfect, but that the current methods of enforcing privacy rights are far superior to prescriptive, comprehensive privacy legislation.

When thinking through the problems they are trying to solve, policymakers should be guided by traditional American understandings of privacy, know how the timing of regulations may impact the economy, and what other state policymakers are proposing.

The timing of regulations will substantially impact the technology ecosystem. As will be discussed later, there are two different approaches to the timing of regulations: *Ex Ante* and *Ex Post*. *Ex ante* regulations—those prescribing actions—may be beneficial when narrowly tailored to address specific privacy concerns. *Ex post* regulations provide the most flexibility for innovative industries, allowing for government oversight by agencies specializing in protecting consumers. Those government agencies may provide frameworks for companies so that the companies can understand what type of conduct is likely to harm consumers and the agencies can punish bad actors.

None of this is to say that policymakers should do nothing. On the contrary, experts have pointed out some weaknesses with current systems. The proposed solutions are diverse, from comprehensive "privacy" legislation dictating what companies must do and say prior to forming the business relationships to narrow laws addressing specific harms. Any decision made will impact innovation, disruption, and the flow of information. Some decisions have the potential to disrupt innovation and the flow of information substantially, stopping them in their tracks. Other decisions will encourage innovation and disruption by providing guardrails and regulatory certainty.

What problem are Policymakers Trying to Solve?

Privacy is an ethereal term. The term tends to mean whatever the speaker or activist wants it to mean.[3] Because of its ethereal nature, activists, academic, and others can use "privacy" and propose any number of solutions without identifying a specific problem the solutions remedy.

> "Policymakers should discern whether 'privacy' concerns are rooted in genuine concerns for consumers or in social distrust of the private sector."

Policymakers should discern whether "privacy" concerns are rooted in genuine concerns for consumers or in social distrust of the private sector—arguments that companies need to fall under the thumb of government regulations because they are "too large" or "grew too large" by exploiting people.[4]

Is the use of, or access to, data a real problem though? Should those that support free markets and limited government cite the monetization of information about a person as a problem? Are policymakers looking at the relationship(s) between consumer and technology platform? Are policymakers considering third-party access to data, either provided by a platform or access entirely independent from a platform?

"Both these factors — the identity of the party collecting information and the nature of the relationship — help address the problem policymakers may be trying to solve."

Each concern is different and ought to demand a different approach. This article primarily examines the relationship between companies and customers. Third party access to data, including the role of data brokers, is an entirely different matter.

There is a plethora of discussions within the company-customer relationship debate. Some argue that people should be able to direct their privacy choices or otherwise own their own data. Some argue that big technology companies are misusing personal data or are profiting on personal data. Still others argue that the risk of identity theft is significant and that companies are not properly securing the data.

The privacy debate is about access to information, specifically information about people. "Privacy", as aptly described by Neil Chilson,[5] is "the result of a limitation on the collection or use of information … [A] person has a degree of privacy when certain information … about that person cannot be *perceived* or *used* by another entity."[6] While a great starting point, the definition leaves out the identity of the party collecting or using the information and the nature of the relationship between the entity collecting the information and the individual. Both these factors — the identity of the party collecting information and the nature of the relationship — help address the problem policymakers may be trying to solve.

Historical American Legal Perspectives on Privacy

American understandings of "privacy" are vastly different from European conceptions. The American understanding primarily looks to government access to data about, or created by, individuals.[7] Americans also have certain expectations that they will be left alone from unwanted intrusions into their personal lives.

The Fourth Amendment to the United States Constitution guarantees that every person will be "secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and that no warrants shall issue, but upon probable cause supported by oath or affirmation…" The Supreme Court has interpreted the Fourth Amendment as providing citizens a "reasonable expectation of privacy"[8] and protecting "people, not places."[9]

This "reasonable expectation" of privacy, though, has some limits. For one, the expectation applies primarily, if not solely, to government surveillance.

> When an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," we have held that *official intrusion* into that private sphere generally qualifies as a search and requires a warrant supported by probable cause.[10]

The American ideas of privacy, while strongly rooted in limitations on government access to information, have some civil application. Starting in the late Nineteenth Century and continuing to the early Twentieth Century, legal scholars and courts proposed, and started to develop, the "privacy" torts. In 1890, Samuel D. Warren and Louis D. Brandeis, who was confirmed

as a Supreme Court Justice in 1916, co-authored a law review article considering "whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual … ."[11]

Since, at the time, there were no "privacy" torts, Warren and Brandeis argued to extend some existing standards to protect a person's privacy. They relied heavily on principles of what we would refer to today as "intellectual property"[12] and to a lesser extent, contract law. From those principles, Warren and Brandeis derived the "right of privacy," which they defined as "the principle which protects personal writings and any other productions of the intellect or of the emotions [extended to protect] the personal appearance, sayings, acts, and to personal relation, domestic or otherwise."[13]

In 1960, by the time Professor William Prosser authored his law review article,[14] privacy law expanded to four categories, which are still applicable today. Those four categories are:

- Unreasonable intrusion upon the seclusion of another;
- Appropriation of another's name or likeness for commercial benefit;
- Unreasonable publicity given to another's private life; and
- Publicity that unreasonably paints another in a false light in the public eye.[15]

Since the law developed in the seventy years after Warren and Brandeis published their article, Professor Prosser was able to analyze all four categories of privacy torts. As may be guessed, each privacy tort has unique elements. Each privacy tort is designed to protect specific interests for people.

According to Professor Prosser, for example, when discussing intrusion upon the seclusion of another, he noted for the tort to apply, "that there must be something in the nature of prying or intrusion… [and] that the intrusion must be something which would be offensive or objectional to a reasonable man."[16]

Unreasonable publicity given to another's private life, or publication of private facts, has a couple elements. To establish a claim, one must prove publication of private facts. "[T]he facts disclosed must be private facts, and not public ones. Certainly, no one can complain when publicity is given to information about him which he himself leaves open to the public eye … ."[17]

A few themes pervade the privacy torts from their inception to modern jurisprudence: publicity, matters made public would be offensive and objectionable to reasonable people, and consent. Consent vitiates any cause of action. If a person consents to the use of his or her photograph in an advertisement, a cause of action for appropriation of likeness cannot be maintained. Similarly, if a person consents to the publication of private facts, even if those facts are highly embarrassing or may damage a person's reputation, actions for false light in the public eye or unreasonable publicity cannot be maintained.

The principle of consent applies to modern data collection, retention, and use. When users of social media platforms voluntarily publish information about themselves, privacy torts do not apply. When individuals voluntarily provide information to social media platforms so that others can access the information, the platform cannot be liable for the information posted by its user. Similarly, when a person posts information on social media platforms or other websites, he or she voluntarily publishes information about himself or herself; or when individuals voluntarily use search engines or sign up for email accounts that costs no money, they voluntarily provide information about themselves to in exchange for the service(s).

Publicity, as a theme, means just that. A matter is publicized through a newspaper, online post, or other manner. It is publicity of a private matter, something that places a person in a false light, the use of a photograph for commercial advantage, or so on. Publicity would mean that the world would know, for example, of a private relationship or an unsavory fact.

The final theme that pervades the privacy torts is that of offensiveness. For the privacy torts to apply, the matter would likely have to be offensive or highly embarrassing. Ordinary fact, or at least average observable facts, are not actionable. "Any one who is not a hermit must expect the more or less casual observation of his neighbors and the passing public as to what he is and does, and some reporting of his daily activities. The ordinary reasonable man does not take offense at mention in a

newspaper of the fact that he has returned from a visit, or gone camping in the woods, or that he had given a party at his house for his friends … ."[18]

The privacy torts do not apply to the broader privacy discussion.[19] Most platforms collect information about individuals directly from the individual with consent, as part of commencing the relationship, or as individuals voluntarily post photographs, status updates, opinions, documents, and so on.

Neither Fourth Amendment jurisprudence nor common law causes of action help elucidate the current "privacy" debate. The foundation certainly helps explain traditional American understandings of privacy and why society values its privacy.

"Reasonable expectations of privacy" apply to government actions. The concepts behind it, though, explain why many Americans simply want to be left alone. Some policymakers cite the "desire to be left alone" as partial justification for regulations that would create barriers companies must jump over prior to the formation of relationships with individuals. Is the mere collection and retention of data, though, a "harm" policymakers should be citing?

Evaluating Consumer Harm and the Timing of Regulations

Constitutional Standards for Harm

When trying to identify a problem to solve, policymakers may do well to ask whether the supposed injury would be recognized by federal courts. The Constitution limits federal court jurisdiction to "cases" and "controversies" arising under the Constitution, federal statutes, or treaties.[20] Federal courts may also hear disputes between citizens of different states if other criteria is met.

When interpreting the Constitution's "cases" and "controversies" standard, the Supreme Court has repeatedly held that plaintiffs must establish "an 'injury in fact' [which is] an invasion of a legally protected interest which is (a) concrete and particularized… and (b) 'actual or imminent, not conjectural or hypothetical.'"[21] The concept of "injury in fact" both predated *Lujan* and the Court built on it afterwards. Some cases have required that the plaintiff "personally suffer some actual or threatened injury,"[22] that the injury be "distinct"[23] or at least not "undifferentiated."[24]

In a 2016 case, the Court was asked to address whether a plaintiff satisfied the "injury in fact" requirement when he alleged that the defendant disseminated incorrect information about him.[25] The Defendant, Spokeo, operated a "people search engine." The plaintiff alleged that, under the Fair Credit Reporting Act, he had a statutory cause of action against Spokeo. The Supreme Court ultimately disagreed for several reasons.

The case has significant implications for the "privacy" debate as it was one of the first where the Court addressed the questions of "informational injury" and standing as applied to the internet and computers. When the Ninth Circuit determined that Robbins had standing, it noted that "'Spokeo violated [Robins'] statutory rights …' and, second, that 'Robins's personal interests in the handling of his credit information are individualized rather than collective.'"[26]

In so stating, the Ninth Circuit focused on the quality of the information Spokeo was offering and how it was handled. The Supreme Court refocused the discussion on whether Robins sufficiently alleged an "invasion of a legally protected interest that [was] concrete and particularized and actual or imminent, not conjectural or hypothetical.'"[27]

> "A legislative body may not supersede the Constitution's injury in fact requirement by creating a right and conferring the ability to sue to potential plaintiffs based on that statutory right."

A legislative body may not supersede the Constitution's injury in fact requirement by creating a right and conferring the ability to sue to potential plaintiffs based on that statutory right. "Article III standing requires a concrete injury even in the con-

text of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III."[28]

When looking at the enacted and proposed state laws regarding privacy, several themes develop. Among the themes is a statutorily created privacy right, which takes any number of forms. Those forms include consumers' "right" to consent to the collection and use of their data, the right to know what type of data companies are collecting down to the minutia of detail, the right to correct inaccurate data, and the right to sue if companies fail to follow the precise letter of the laws and proposals.

Unclear is whether any of these rights recognize an injury in fact.[29] At least one federal court applying the *Lujan* and *Spokeo* precedents has concluded that the mere collection and retention of data, even without the consumer's express consent or knowledge, cannot be an injury-in-fact.[30]

The injury-in-fact standard should give policymakers pause to reflect, again asking the question of "what harm are we trying to solve?" *Spokeo* and *Rivera* simply stand for the proposition that policymakers ought not focus merely address the collection and retention of data, when identifying a harm.

The problems policymakers must identify, instead, should be the collection and use of data, plus some other harm. In this, policymakers must choose: either the problem is corporate access to and use of information about consumers, including information the consumers voluntarily create, or something else like the risk of identity theft, the risk that the data collectors may not employ commercially reasonable security standards, that data collectors obtain information about consumers by deceiving consumers about the use of data, and so on. Depending on how policymakers perceive the problem, the solutions will broadly vary.

Timing of Regulations, Ex Ante or Ex Post?

There are two basic approaches to the timing of policies: *ex post* and *ex ante*. *Ex ante* regulations are laws or regulations that "take effect before the regulated actor's conduct occurs" while *ex post* regulations are those taking effect "after the conduct occurs."[31] Neither approach is perfect. Both approaches have their advantages and disadvantages. One approach, though, tends to be more flexible which allows for technology to grow.

Ex ante regulations "are almost exclusively a matter of conjecture."[32] When policymakers adopt an *ex ante* approach, they try to guess the negative externalities of a particular action and command avoidance of them.[33] *Ex ante* "regulation is implemented before the external harm or benefit actually happens, usually around the time that important economic decisions are being made."[34]

Examples of *ex ante* privacy regulations include California's Consumer Privacy Law ("CCPA")[35] and Europe's General Data Protection Regulation (GDPR). *Ex ante* regulations heavily regulate what companies can do with information or what they must do prior to collecting data from potential users. "In the case of privacy regulations [*ex ante*], this can mean banning or fining certain information uses, requiring that private entities cease the use of information on demand, or mandating

"Both *ex post* and *ex ante* approaches assume there is some market failure that needs to be corrected. The question is whether policymakers want to defer more to market-action or government-action. *Ex ante* relies heavily on government oversight while *ex post* defers heavily to the private sector."

that private entities seek permission before rolling out new uses of stored information."[36]

Ex post regulations are those regulations enforced after a violation or harm occurs. When policymakers adopt an *ex post* approach, they establish behavioral standards and then act after consumers are harmed. *Ex post* regulation is implemented after the external harm or benefit happens, which can be months or years later.

Examples of *ex post* privacy regulations include the Federal Trade Commission's ("FTC") current approach to privacy and data security. When the FTC started exerting jurisdiction over online consumer privacy issues in the mid-1990s, it "initially encouraged self-regulation. Instead of the FTC creating rules, the companies themselves would create their own rules, and the FTC would enforce them. The FTC would thus serve as the backstop to the self-regulatory regime, providing it with oversight and enforcement."[37]

Both *ex post* and *ex ante* approaches assume there is some market failure that needs to be corrected. The question is whether policymakers want to defer more to market-action or government-action. E*x ante* relies heavily on government oversight while *ex post* defers heavily to the private sector.[38]

Policymakers can use either the *ex ante* approach, the *ex post* approach, or a combination of both. There are examples of narrowly tailored *ex ante* laws effectively protecting consumer privacy. Some of these examples include the Children's Online Privacy Protection Act (COPPA),[39] the Health Insurance Portability and Accountability Act (HIPAA),[40] and the Fair Credit Reporting Act (FCRA).[41]

The timing of regulations may have significant impacts on innovation, disruption, the flow of information, and a state's e-commerce marketplace. Comprehensive, *ex ante* prescriptions may have significant negative externalities. Since the mid-1990s, the United States has led in online disruption and innovation largely because federal legislators chose to apply primarily *ex post* regulations to the burgeoning industry. Comparing the results of comprehensive *ex ante* regulations in Europe with the existing *ex* post regulatory scheme in the United States may help illustrate this proposition.

Analyzing Existing and Proposed Laws

Complying with existing privacy laws reduces innovation, places huge compliance burdens on companies, and subjects companies to litigation and potentially significant fines. The combination of these factors favors incumbent providers, securing market share for them by forcing potential disruptors and competitors out of the market.

Many of the laws and proposals dictate what conditions must be present when companies and consumers make economic decisions. In some cases, such as biometric information privacy laws, the laws are supposedly narrowly-tailored to address one specific type of perceived problem. But even narrowly-tailored laws may have unintended consequences with, for example, both Facebook and Google facing lawsuits for implementing facial recognition software.

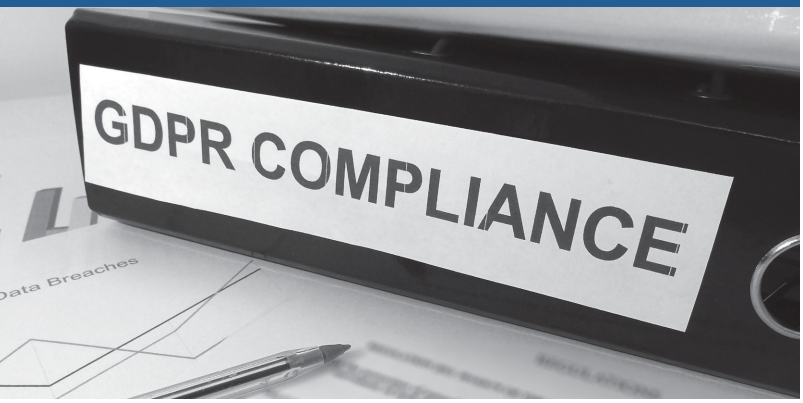
California's privacy law and all state privacy proposals would establish a patchwork of privacy laws for people, companies, and others to comply with. While there are similarities between the provisions, there are substantial differences. If one state copies, word for word, the proposal of another state, there is no guarantee that regulators or courts of those two states would interpret the provisions entirely. Because the laws and proposal inevitably force companies outside the state to comply with the standards — even if those companies barely do business in the regulating state — it is unclear whether such regulations are permissible under the Dormant Commerce Clause.[42]

California and Europe, as well as many of the state proposals, seem to operate from the perspective that the "privacy problem" is rooted in the private sector. The laws focus heavily on corporate behavior and establish fines, or at least ways to calculate fines, when companies fail to fulfill every jot-and-tittle of the law prior to collecting information about individuals.

Europe's General Data Protection Regulation

Proponents of Europe's GDPR claimed that the scheme would give "citizens more control over their personal information"[43] by limiting "tech firms' powers."[44] The regulatory regime requires, among other things, that companies "[a]llow customers to see

"Both European and American businesses have spent considerable sums complying with the regime. According to at least one report, "British firms have now sunk a combined $1.1 billion preparing for GDPR" while their American counterparts have spent "a whopping $7.8 billion." For American companies, that is $7.8 billion spent on compliance that could have been used to hire new engineers, reinvest in research and development, or invest in other capital projects."



and delete the data that concerns them," "[m]ake data policies transparent to an average person (i.e. don't hide privacy stuff in legalese no one reads)," and "[h]ire a Chief Data Officer in some cases."[45] GDPR threatens significant fines for companies that fail to comply with the rules, "up to 4% of its global turnover or $20 [million] euros ($23.4 million), whichever is higher."[46]

Rather than promoting "privacy," GDPR has restricted the flow of information to Europe, hampered innovation, and lead to United States' companies sinking millions, if not billions, of dollars into compliance costs. Many United States' newspapers either cut or significantly curtailed services to Europe, including the Los Angeles Times, the Chicago Tribune, and hundreds of local papers.[47]

Innovators are feeling the pinch, too. While many of them take economic risks others would not, innovators are simply not willing to risk running afoul of GDPR.[48] Several small businesses and innovators announced they would shutter European operations when GDPR became effective including a mobile marketer, an online gaming company, and a social network for classmates, to name a few.[49]

Both European and American businesses have spent considerable sums complying with the regime. According to at least one report, "British firms have now sunk a combined $1.1 billion preparing for GDPR" while their American counterparts have spent "a whopping $7.8 billion."[50] For American companies, that is $7.8 billion spent on compliance that could have been used to hire new engineers, reinvest in research and development, or invest in other capital projects.

Not surprisingly, the companies that can most afford to comply with GDPR are the incumbent technology giants. They "are better positioned to absorb the significant costs of compliance."[51] They are also positioned to reap the economic benefits of a heavily-regulated market with one online advertising giant seeing its market share in Europe increase from 50 percent of online revenues to almost 95 percent the "first day after the rules took effect."[52]

California Privacy

California's privacy law tries to mimic GDPR.[53] The law, entitled the California Consumer Privacy Act,[54] is significantly flawed[55] and includes typographical errors given the short duration the legislature had to debate and pass the proposal.[56] Yet, despite those flaws, many of the proposals introduced in other states try to copy it.

Because many state proposals try to copy California's law, it is worth briefly summarizing what the law tries to do. According to Professor Eric Goldman, the law:

> Imposes 6 new obligations on covered businesses: they have to make specified disclosures to consumers, provide consumers with a data erasure capacity, provide consumers with data portability, allow con-

sumers to opt-out of data sales (or opt-in in the case of minors), and not discriminate against consumers on the basis of personal information. The law also creates a private cause of action for certain data breaches.

Similarly, proponents of the ballot measure that forced the legislature's hand claimed the law would provide consumers the "1. Right to know *all* data collected by a business on you, twice a year, free of charge. 2. Right to say *no* to the sale of your information. 3. … Right to sue companies who collect your data… if the company was careless or negligent about how it protected your data … 4. Right to *delete* data you have posted …" and so on.[57]

While the privacy law tries to mimic GDPR, there are similarities and differences. The International Association of Privacy Professionals compared the two laws and summarized the synergies and differences.[58] The report noted that both the California law and GDPR "extend well beyond the physical borders of their respective jurisdictions." Most of the differences, according to the report, relate to definitions and limitations. For example, the definition of "personal data" is far broader in the California privacy law than for GDPR, but California does "not contain data processing principles" or restrictions on what can be done "internally with personal data," while GDPR contains, at least, some limitations.

Professor Goldman noted several problems with the law including that it "covers too many enterprises."[59] The law identifies tech giants such as Facebook and Google as problematic, but the impact will be primarily borne by innovators, mom-and-pop shops, and other small businesses. In a quest to punish technology giants for succeeding too much, as defined by the government and activists, the law will help the giants grow in power and market share at the expense of smaller businesses.

Existing privacy laws such as California's Consumer Privacy Act and GDPR demonstrate the negative consequences of focusing on corporate behavior, or the private sector, as the problem in need of solving rather than focusing on consumers and trying to remedy consumer harm. The proposals overreach their targets, insulate incumbents, prevent the free flow of information, and suppress innovation.

State Biometric Information Privacy Laws

Most states have not adopted privacy laws. The debate is growing as a number of policymakers have introduced proposals. A few states have laws regulating what companies must do to obtain residents' biometric information, including Illinois, Texas, and Washington.

Operationally, the three states typically refer to specific "biometric identifiers", building the regulations around what companies can, or cannot, do with the information. The definitions vary from broad to specific. Texas, for example, defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry."[60]

Compare Texas's definition to Washington's definition, which is more comprehensive. Washington defines "biometric identifier" as "data generated by automatic measurements of an individual's biological characteristics, such as fingerprint, voiceprint, eye retinas, irises, or other unique biological patters or characteristics that is used to identify a specific individual."[61]

The laws range from prohibitive to permissive. Some experimentation is permitted in states like Texas, while companies may be punished for trying new services in Illinois.[62]

Illinois's law entitled the Biometric Information Privacy Act[63] effectively prohibits entities, such as Facebook or Google, from implementing facial recognition technology. The statute allows both the state attorney general and members of the public, through a statutory right of action, to enforce the law. Among other requirements, BIPA:

- Requires private entities … to obtain consent from a person before collecting or disclosing their biometric identifiers.
- Requires private entities that possess such identifiers to timely destroy them: when the purpose of collection ends, and in no event more than three years after the last contact with the subject.
- Requires private entities to securely store such identifiers.

- Allows parties injured by violations of these rules to file lawsuits to hold businesses accountable.[64]

Texas's law entitled Capture or Use of Biometric Identifier[65] prohibits the "capture [of] biometric identifier[s] … for commercial purpose[s] unless …" the private entity informs the individual that the information is being captured and obtains his or her consent. The law is slightly more permissive than Illinois's law as only the attorney general in Texas may bring an enforcement action, but the potential consequences are statutorily much higher than Illinois.[66]

Finally, unlike Illinois and Texas, Washington law does not have a specific name.[67] The law is closer to that of Texas than to Illinois. As with Texas, Washington requires companies to provide notice and obtain consent from consumers prior to collecting the data. Both Washington and Texas require companies to take "reasonable care to guard against unauthorized access to and acquisition of biometric identifiers"[68] and limits enforcement to the attorney general under the state's consumer protection laws.[69]

State Legislative Proposals

As of the writing of this paper, only California has enacted statewide privacy legislation.[70] A few other states have introduced privacy legislation.[71] Some state proposals are modeled after California's privacy law while other proposals are independent.

While biometric privacy laws are not pure analogues to online privacy, the *ex ante* restrictions regarding the use and collection of data both place on companies have similar consequences. Both online privacy and biometric privacy laws have substantial impacts on innovation and disruption. Facebook and Google for example, are faced or are facing legal challenges in Illinois because of their facial recognition software.[72] These lawsuits deter innovators, both large and small, from operating in the state. The lawsuits also do not account for the risk of fines, investigations, or other actions state attorneys general may take.

Comprehensive privacy proposals have been introduced in several states, including Hawaii,[73] Massachusetts,[74] Mississippi,[75] New Mexico,[76] New York,[77] North Dakota,[78] and Washington.[79]

"Many of the proposals lack specificity, and because they share several definitions in common, this is a problem across all the proposals. For example, the original text of Mississippi's House Bill 1253 stated that it was the legislature's intent to prevent 'the unauthorized disclosure of personal information.'"

Democrats control the legislative and executive branches in most of these states and most of the proposals are spearheaded by Democrats. The exceptions to Democratic control are Mississippi and North Dakota. In North Dakota, the effort to enact privacy legislation was led by a Republican.

The proposals are not really focused on privacy, but on disrupting the relationship between a product or service provider and the people who need or want services. That is, the proposals assume the problem they need to solve is corporate access to, and use of, data. As such, the proposals are focused on corporate behavior, not on consumers. If the proposals focused on consumers, the proposals would recognize the benefits many of the services provide to consumers and would focus, instead, on remedying harms consumers suffer from the misuse of personal information.

Many of the proposals have similar provisions and definitions. Many of the proposals lack specificity, and because they share several definitions in common, this is a problem across all the proposals. For example, the original text of Mississippi's House Bill 1253 stated that it was the legislature's intent to prevent "the unauthorized disclosure of personal information." But the language of the proposal was unclear. Did the legislature intend to ameliorate the risk of hacking, prohibit the disclosure of information to third parties without consumer consent, or simply point to the potential vulnerability of data?

Hawaii's proposal includes a vague definition of consumer. It

defines a consumer as "an individual who interacts with a business within the state." Does the business have to be within the state? If the business is not located in the state, the provision would seem to run afoul of the Dormant Commerce Clause. What does the legislature mean by "interacts"? Is this a physical or digital interaction? Does the interaction have to be for the purpose of commerce?

New Mexico's proposal is unclear as to how often businesses must provide notice before collecting information. Under the proposal, businesses must *"[a]t the time of or before collection* of personal information … provide notice to the consumer …" (emphasis added). The text would seem to indicate businesses must obtain consumer consent every time before collecting information. This would mean before New Mexico residents visit Amazon, Gmail, Facebook, or even the websites of New Mexico businesses, he or she would be forced to read through and consent to long disclosures.

New York's proposal is so vague that it would include anyone who "in the course of their *personal*, business, commercial, corporate … operations collects, *receives*, stores, maintains, processes, or otherwise *has access to* personal information." (Emphasis added.) With an equally broad definition of "personal information," the proposal could subject anyone who receives an email in New York to the state's privacy proposal.

"New York's proposal is so vague that it would include anyone who 'in the course of their personal, business, commercial, corporate … operations collects, receives, stores, maintains, processes, or otherwise has access to personal information.'"

All the proposals erect huge barriers to entry and obstacles for companies to overcome prior to offering services in the states. The proposals apply equally to in-state and out-of-state businesses if they meet certain thresholds. These obstacles include:

- Creating a process for verifying consumer requests for information, and specifically requests to know what type of information the company collects about the consumer, what type of categories the company breaks the information into, and to what entities the companies may sell the information;
- Requiring companies to respond to verified requests for information within a set time period, often 45 days;[80]
- Requiring companies to post extensive disclosures about the information they collect, why they collect various categories of information, the companies with which they do business, and more before individuals can consent to the collection of information;
- Prohibiting companies from denying services if a person opts-out of the information collecting practices or from discriminating by providing a lesser service to those people; and
- Allowing residents of the state to sue the companies if they believe the companies violate the law, and provides either for attorney's fees, statutory damages, or both.

Nearly all the proposals would require "covered entities," whether companies or individuals as provided by the language, to provide notice to the consumer regarding the data collection practices and obtain the consumer's consent. The notices provided according to the proposals would need to include a lot of information, such as:

- The categories of personal information to be collected and the purposes for which the categories of personal information will be used;
- Whether the information might be sold and that the consumer has a right to opt out of the sale of the personal information;

- The business purpose(s) for third party disclosure; and

- Consumers' rights to request information.[81]

When a consumer submits a verified request for disclosure to a "covered entity" or business the proposals require it to respond with more information than required during the "notice-and-consent" period. For example, Hawaii's proposal would require a covered entity or business to disclose:

> [I]dentifying information that the business has collected about the consumer, including
>
> (1) The categories of identifying information the business has collected about the consumer;
>
> (2) The sources from which the identifying information about the consumer has been collected;
> (3) The specific pieces of identifying information that the business has collected from the consumer;
>
> (4) The business or commercial purposes for collecting or sharing the identifying information; and
>
> (5) The categories of third parties with whom the business has shared identifying information about the consumer.[82]

A few of the proposals limit or prohibit the collection or use of biometric information. [83] This includes the inability to use facial recognition software without individuals' consent, though the face is the most common way for people to identify each other.[84]

A few of the proposals also permit the state attorney general, government commissions, or other governmental entity to pursue companies that violate the law, promulgate additional rules under the section, or both. For example, the New Mexico proposal would allow the state attorney general to establish additional criteria for "biometric information" and issue advisory opinions to help guide compliance.[85] Similarly, at least one New York proposal would require companies to submit "comprehensive security programs" for approval by the office of information technology services.[86]

The farthest-reaching proposal was probably that of Washington State.[87] The proposal varies significantly both from California's Privacy Law and many of the state proposals. Washington State rather overtly attempted to codify GDPR within state law, which would have had disastrous consequences for innovation, small businesses, and even individuals seeking to browse the internet.

The proposal referenced GDPR positively and stated that "Washington residents deserve to enjoy the same level of robust privacy safeguards."[88] The proposal also praised the benefits of innovation and technology.

As with many of the other state proposals, the proposal applied to "legal entities that conduct business in Washington or produce products or services that are intentionally targeted to residents of Washington, and … (a) Controls or processes personal data of one hundred thousand consumers or more; or (b) Derives over fifty percent of gross revenue from the sale of personal data and processes or controls personal data of twenty-five thousand consumers or more."

If enacted, the proposal would have required those businesses, regardless of whether they are in Washington State, to expend significant resources complying with the law's demands. Immediately after the definitions and jurisdictional statement, the proposal required all entities satisfying the jurisdictional statement to establish and hire personal data "Controllers." Controllers would have several responsibilities, including complete compliance with the law, which included provisions like those discussed for other states, such as receiving verified requests from consumers and providing them with information regarding the data collected about them.

The Washington State proposal, though, added a new wrinkle to the responsibilities of controllers and the "rights" of consumers. Consumers could object to the information collected about them and demand that the company correct any "inaccurate personal data" and delete data the consumer believed "there [is] no business purpose for processing."

Controllers would have been required to conduct "risk assessments." Those risk assessments must "identify and weigh the benefits that may flow directly and indirectly from the process-

ing [of the data] … against the potential risks to the rights of the consumer associated with such processing …" If the potential risk to privacy outweighed the benefit, the business would need to obtain the consent of the consumer prior to processing. The business would need to keep the assessment on file and provide it to the attorney general "upon request." In other words, the proposal would have required the business to justify why it collects data and submit the business case to the government, upon request.

State privacy proposals are aimed at regulating corporate conduct, rather than addressing consumer harms. They all identify the private sector as the problem policymakers need to "solve." The proposals ignore the fact that the private sector is already responding to the demands of consumers, creating tools to help them manage their information.[89]

The Consumer Protection Model

A single, federal standard is ideal for laws or regulations. Until Congress passes such a law, though, policymakers should consider a framework that both promotes innovation and protects consumers. Most states, and the federal government, already have that positive framework in place. That framework authorizes state attorneys general and the Federal Trade Commission to pursue any company engaging in a fraudulent and deceptive trade practices.[90]

States and the federal government share joint, and often concurrent, consumer protection jurisdiction.[91] State consumer protection laws, generally, fall into one of two broad categories: those that prohibit unfair and deceptive practices; and those that proscribe deceptive trade practices.[92] All states have laws proscribing deceptive trade practices,[93] while a small number of states also have laws proscribing unfair trade practices.[94]

The former point — that all states prohibit deceptive trade practices — is critical. Most companies offering services or products to people through the internet have terms of service, privacy policies, and other similar documents posted on their websites. Through these documents, companies make representations and promises to individuals regarding specific standards, including the use of consumer data. If a company breaches its agreements or misrepresents how it uses data, state and federal consumer protection agencies can act to protect disaffected consumers without comprehensive privacy laws.[95]

States are free to bring their own enforcement actions, often through their state's attorney general, against companies that

"The FTC and state attorneys general are well-positioned to identify and solve actual harms to privacy — whether breached contracts, data breaches, and so on. The current consumer-harm focused system can both keep the private sector accountable and provide the flexibility necessary to promote innovation."

violate representations made to consumers.[96] State consumer protection laws may also permit private causes of action brought by disaffected consumers or companies.[97] States may elect to follow FTC standards for deceptive trade practices or they may craft their own standards.[98] Some states have elected to follow the FTC standards of the 1980s, which defines unfairness as "conduct that 'offends public policy,' 'is immoral, unethical, oppressive, or unscrupulous,' and 'causes substantial injury to consumers."[99] A minority of states shifted with the FTC in 1980, when it "shifted the focus of the federal test primarily to the substantial consumer injury component, making it significantly more difficult for the government to establish a violation."[100]

The FTC and state attorneys general are well-positioned to identify and solve actual harms to privacy — whether breached contracts, data breaches, and so on. The current consumer-harm focused system can both keep the private sector accountable and provide the flexibility necessary to promote innovation.

This is not to say the current system is perfect. Policymakers could examine the current system and see where there is room for improvement. For example, should governments have a role promoting increased transparency regarding terms of service or should governments have a role protecting consumers from ever-changing terms of service?

Conclusion

California's privacy law and the current proposed privacy laws in states fail to identify actual harms to consumers. Instead, they rely on conjectural harms rooted in a distrust of the private sector. The proposals substitute the government's judgment for consumer choice. The proposals will do little to address the "problems" of privacy by insulating the current incumbents from competition while reducing consumer choice and innovation.

Privacy is an ethereal concept. The term currently means whatever activists, policymakers, and others want it to mean. That definition may be rooted in the traditional American understanding of privacy, or it may not be.

Policymakers should look identify actual harms to consumers and figure out solutions to those actual harms. Those solutions may take the form of limited *ex ante* prescriptions, as in the case of HIPAA or COPPA; *ex post* regulations that react to violations of contract or representations, as in the case of the Federal Trade Commission's current privacy enforcement regime; or a bit of both.

The current *ex post* approach to privacy enforcement has led to the explosion of the online ecosystem, adding trillions of dollars in value to the economy, creating hundreds of thousands of high-paying jobs, and providing services in high demand. Comprehensive privacy legislation could hamper, or even destroy, this vibrant online ecosystem.

State consumer protection agencies and attorneys general can look to the FTC for guidance. Until federal legislation is enacted, state attorneys general can supplement the FTC's enforcement using state consumer protection laws. State policymakers would do well to look to existing frameworks, questioning whether they are sufficient before contemplating comprehensive legislation.

Endnotes

1 E.g. Antonio Garcia Martinez, *No Data is Not the New Oil*, Wired, February 26, 2019. Available at https://www.wired.com/story/no-data-is-not-the-new-oil.

2 *Compare*, Neil Chilson, *When Considering Federal Privacy Legislation*, Regulatory Transparency Project of the Federalist Society, December 4, 2018. Available at https://regproject.org/wp-content/uploads/RTP-Cyber-Privacy-Working-Group-Paper-Privacy-Legislation.pdf.

3 *See* Adam Thierer, *The Pursuit of Privacy in a World Where Information Control is Failing*, Harvard Journal of Law & Public Policy Vol. 36 No. 2 (2013), 409-455, 415. ("[P]rivacy has always been a highly subjective philosophical concept. It is also a constantly morphing notion that evolves as societal attitudes adjust to new cultural and technological realities. For these reasons, America may never be able to achieve a coherent fixed definition of the term or determine when it constitutes a formal right outside of some narrow contexts.") Available at https://www.mercatus.org/system/files/The-Pursuit-of-Privacy-Adam-Thierer.pdf.

4 *See*, *e.g.*, *Media Capitalism, the State and 21st Century Media Democracy Struggles: An Interview with Robert McChesney*, The Bullet No. 246, Aug. 9, 2009. Available at https://www.socialistproject.ca/bullet.246.php. ("The final issue that we have to deal with… is what I call hyper-commercialism. This is the conversion of every space and moment of time in our lives to selling something, promoting something, branding something… As the internet is increasingly hyper-commercialized, we open our entire lives to 24/7 injections of advertising messages. We need to organize against hyper-commercialism…" and "We are at a critical juncture in the history of communication. The world economic crisis is accentuating that critical juncture because it impacts all of society. The capitalist economy dominated by corporations has failed.) Farhad Manjoo, *Tackling the Internet's Central Villain: The Advertising Business*, The New York Times, Jan. 31, 2018. Available at https://www.nytimes.com/2018/01/31/technology/internet-advertising-business.html. (Calling for greater government regulation of the technology industry, including online advertising and data collection. The article also links the anti-free market calls for regulation to the "privacy" debate.)

5 Former acting Chief Technologist for the Federal Trade Commission and currently a senior research fellow for technology and innovation with the Charles Koch Institute.

6 Chilson, *When Considering Federal Privacy Legislation*, cited above (emphasis original).

7 *See broadly*, Robert D. Richards, *Compulsory Process in Cyberspace: Rethinking Privacy in the Social Networking Age*, Harvard Journal of Law & Public Policy Vol. 36, No. 2, 519-548 (2013)

8 E.g. *Katz v. United States*, 389 U.S. 347, 360-361 (1967) (Harlan, J., concurring).

9 *Carpenter v. United States*, ___ U.S. ___, 138 S.Ct. 2206, 2213 (2018)

10 *Carpenter*, 138 S.Ct. at 2213, *citing Smith v. Maryland*, 442 U.S. 735, 740 (1979) (emphasis added).

11 Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220, 197. Available at https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

12 "It is not however necessary, in order to sustain the view that the common law recognizes and upholds a principles applicable to cases of invasion of privacy… for the legal doctrines relating to infractions of what is ordinarily termed the common-law right to intellectual and artistic property are… but instances and applications of a general right to privacy…." *The Right to Privacy*, above, p. 197.

13 *The Right to Privacy*, above, at p. 213.

14 William L. Prosser, *Privacy*, 48 Calif. L. Rev. 383 (1960). Available at https://scholarship.law.berkeley.edu/californialawreview/vol48/iss3/1/.

15 Restatement (Second) of Torts, §§ 652A-E (1977).

16 *Privacy*, above, pp. 390-391.

17 *Privacy*, above, p. 394.

18 *Privacy*, above, pp. 396-397.

19 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, Columbia Law Rev. 114 (2014): 583-676, 590-591. Available at https://columbialawreview.org/wp-content/uploads/2016/04/Solove-Hartzog.pdf. Hereafter "Solove, *FTC and Privacy Common Law*."

20 U.S. Const. Art. III Sec. 2.

21 *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992) (internal citations omitted). The Court further added that "there must be a causal connection between the injury and the conduct complained of—the injury has to be 'fairly…traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court.' Third, it must be 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" *Id*. at 560-561.

22 *Valley Forge Christian College v. Americans United for Separation of Church and State, Inc.*, 454 U.S. 464, 472 (1982)

23 *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990).

24 *United States v. Richardson*, 418 U.S. 166, 177 (1974).

25 *Spokeo Inc. v. Robins*, 578 U.S. ___, 136 S.Ct. 1540 (2016)

26 *Spokeo*, 136 S.Ct. at 1544.

27 *Spokeo*, 136 S.Ct. at 1548 (internal quotations omitted). The Court also noted that "concrete" is not synonymous with "tangible." Intangible injuries, according to the Court "can nevertheless be concrete." *Id*. at 1549.

28 *Spokeo*, 136 S.Ct. at 1549.

29 *Spokeo* would seem to be immediately relevant to those states that include in their proposals the right to correct "inaccurate information." It is unclear how an individual may be harmed when a technology platform has collected inaccurate information, as the inaccurate information is not likely to form the basis of any consequential decision, such as the extension of credit.

30 *Rivera v. Google*, E.D. Ill. 2018. Available at https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2880&context=historical.

31 Kyle D. Logue, *In Praise of (Some) Ex Post Regulation: A Response to Professor Galle*, Vand. L. Rev. En Banc 69 (2016): 97-122. Available at https://repository.law.umich.edu/cgi/viewcontent.cgi?article=2752&context=articles. Hereafter "Logue, *In Praise of (Some) Ex Post Regulation*."

32 *Ex Post v. Ex Ante Regulatory Remedies Must Consider Consumer Benefits and Cost*, American Consumer Institute, May 14, 2008. Available at http://www.theamericanconsumer.org/2008/05/ex-post-v-ex-ante-regulatory-remedies-must-consider-consumer-benefits-and-costs/.

33 Andrea O'Sullivan, *How to Promote Data Privacy While Protecting Innovation*, The Bridge, Mercatus Center at George Mason University, February 13, 2019. Available at https://www.mercatus.org/bridge/commentary/how-promote-data-privacy-while-protecting-innovation?utm_source=marketing&utm_medium=email&utm_campaign=issuespotlight.

34 Logue, *In Praise of (Some) Ex Post Regulation*, 107.

35 Cal. Civ. Code §§ 1798.100, *et seq*.

36 O'Sullivan, *How to Promote Data Privacy*, above.

37 Solove, *FTC and Privacy Common Law*, 598.

38 Logue, *In Praise of (Some) Ex Post Regulation*, 102, 108. ("The strength of ex post approach is that it asks less of the government regulator. This is so in the following sense: the regulator—whether it is an agency or a court—must determine the extent of the harm caused by the regulated party's activity only after the harm has occurred.")

39 15 U.S.C. §§ 6501-6506.

40 *E.g.* 42 U.S.C. § 1320d-6 (Wrongful disclosure of individually identifiable health information).

41 15 U.S. C. §§ 1681-1681u.

42 The Dormant Commerce Clause, or the "'negative' aspect to the Commerce Clause [ ] limits the power of states to regulate interstate commercial activities." The Dormant Commerce Clause, because it is a constitutional provision, ensures the "ability of individuals to engage in commerce free of unduly burdensome or protectionist state regulation." *See*, Norman R. Williams, *Why Congress May Not "Overrule" the Dormant Commerce Clause*, 53 UCLA L. Rev. 153 (2005). Available at https://www.uclalawreview.org/why-congress-may-not-overrule-the-dormant-commerce-clause/. It is worth noting that one of the California law's authors admitted the law would reach beyond the state's borders, establishing a *de facto* national standard. "I think it's going to set the standard across the country that legislatures across the country

will look to adopt in their own states." Tony Romm, *California legislators just adopted tough new privacy rules targeting Facebook, Google and other tech giants*, The Washington Post, June 28, 2018. Available at https://www.washingtonpost.com/technology/2018/06/28/california-lawmakers-just-adopted-tough-new-privacy-rules-targeting-facebook-google-other-tech-giants/. Beyond this paragraph and footnote, whether such privacy laws and proposals violate the Dormant Commerce Clause is beyond the scope of this paper.

43 Chris Morris, *These U.S. Media Sites Have Gone Dark in Europe as New GDPR Rules Kick In*, Fortune, May 25, 2018. Available at http://fortune.com/2018/05/25/gdpr-us-media-sites-not-accessible/.

44 *GDPR: US news sites unavailable to EU users under new rules*, BBC News, May 25, 2018. Available at https://www.bbc.com/news/world-europe-44248448.

45 Jeff John Roberts, *GDPR Is in Effect: Should U.S. Companies Be Afraid?* Fortune, May 25, 2018. Available at http://fortune.com/2018/05/24/the-gdpr-is-in-effect-should-u-s-companies-be-afraid/.

46 Morris, *These U.S. Media Sites Have Gone Dark*.

47 *E.g.* Morris, *These U.S. Media Sites Have Gone Dark*. *See also*, Andrea O'Sullivan, *The EU's New Privacy Rules Are Already Causing International Headaches*, Reason, June 12, 2018. Available at https://reason.com/archives/2018/06/12/the-eus-new-privacy-rules-are-already-ca.

48 O'Sullivan, *How to Promote Data Privacy*, above.

49 Ivana Kottasova, *These companies are getting killed by GDPR*, CNN, May 11, 2018. Available at https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html.

50 Oliver Smith, *The GDPR Racket: Who's Making Money from this $9bn Business Shakedown*, Forbes, May 2, 2018. Available at https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#11c5d5fd34a2.

51 Adam Thierer, *How Well-Intentioned Privacy Regulation Could Boost Market Power of Facebook & Google*, The Technology Liberation Front, April 25, 2018. Available at https://techliberation.com/2018/04/25/how-well-intentioned-privacy-regulation-could-boost-market-power-of-facebook-google/.

52 O'Sullivan, *The EU's New Privacy Rules*, above.

53 *California's new online privacy law could be huge for the US*, MIT Download, June 29, 2018. Available at https://www.technologyreview.com/the-download/611570/californias-new-online-privacy-law-could-be-huge-for-the-us/.

54 Cal. Civ. Code §§1798.100, *et seq.* Available at https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=.

55 E.g. Tony Romm, *Inside the lobbying war over California's landmark privacy law*, The Mercury News, February 9, 2019. Available at https://www.mercurynews.com/2019/02/09/californias-landmark-privacy-law-sparks-lobbying-war-that-could-water-it-down/; Robert Callahan, *California privacy law must be changed to avoid making user data more vulnerable*, The Sacramento Bee, December 19, 2018. ("The law was passed last summer with the idea that it would be amended and fixed in 2019. The Internet Association, on behalf of the companies we represent, has been working with the California Legislature and other stakeholders to find reasonable solutions to CCPA's substantive problems. These problems were given short shrift during the extreme rush to pass the law, but now must be addressed.") Available at https://www.sacbee.com/opinion/op-ed/article223327375.html.

56 Eric Goldman, *A Status Report on the California Consumer Privacy Act*, Technology & Marketing Law Blog, February 14, 2019. Available at https://blog.ericgoldman.org/archives/2019/02/a-status-report-on-the-california-consumer-privacy-act.htm.

57 *About the California Consumer Privacy Act*, Californians for Consumer Privacy. Available at https://www.caprivacy.org/about. (Emphasis original.)

58 Lydia de la Torre, *GDPR matchup: the California Consumer Privacy Act 2018*, IAPP, July 31, 2018. Available at https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/.

59 Eric Goldman, *The California Consumer Privacy Act Should be Condemned, Not Celebrated*, Technology & Marketing Law Blog, August 9, 2018. Available at https://blog.ericgoldman.org/archives/2018/08/the-california-consumer-privacy-act-should-be-condemned-not-celebrated-cross-post.htm.

60 Texas Bus. & Commerce Code §503.001(a). Available at https://codes.findlaw.com/tx/business-and-commerce-code/bus-com-sect-503-001.html.

61 19 RCW 375.010(1).

62 *E.g.* Russell Brandom, *Crucial biometric privacy law survives Illinois court fight*, The Verge, January 26, 2019. Available at https://www.theverge.com/2019/1/26/18197567/six-flags-illinois-biometric-information-privacy-act-facial-recognition. *Compare* Shannon Liao, *Google wins dismissal of facial recognition lawsuit over biometric privacy act*, The Verge, December 29, 2018. Available at https://www.theverge.com/2018/12/29/18160432/google-facial-recognition-lawsuit-dismissal-illinois-privacy-act-snapchat-facebook.

63 740 ILCS 14/1, *et seq.* Available at http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004.

64 Adam Schwartz, *New Attack on the Illinois Biometric Privacy Act*, Electronic Frontier Foundation, April 10, 2018. Available at https://www.eff.org/deeplinks/2018/04/new-attack-illinois-biometric-privacy-act.

65 Texas Bus. & Commerce Code §503.001.

66 Jerri Lynn Ward, J.D., *Texas Biometric Privacy Law restricts certain "biometric identifiers,"* GarloWard, P.C., March 26, 2018. Available at https://www.garloward.com/2018/03/26/texas-biometric-privacy-law-restricts-certain-biometric-identifiers-three-states-laws-regulating-collection-storage-biometric-data/.

67 19 RCW §§ 375.010, *et seq*.

68 *E.g.* 19 RCW §375.020(4)(a).

69 19 RCW 375.030(2).

70 Odia Kagan, *Multiple States Considering New Data Privacy Legislation*, Privacy Compliance & Data Security, Fox Rothschild, February 10, 2019. Available at https://dataprivacy.foxrothschild.com/2019/02/articles/california-consumer-privacy-act/multiple-states-considering-new-data-privacy-legislation/.

71 This paper addresses privacy proposals impacting the relationship between individuals and companies. Since the Congressional Resolution disapproving of the FCC's privacy rules was enacted in (2017), several states introduced ISP Privacy Laws. While those privacy laws are tailored to a specific industry, they are outside the scope of this paper.

72 *See, e.g.,* Jeff John Roberts, *Court's Biometric Ruling Poses Billion Dollar Risk to Facebook, Google*, Fortune, January 28, 2019. Available at http://fortune.com/2019/01/28/facebook-face-scanning-bipa/. Russell Brandom, *Crucial biometric privacy law survives Illinois court fight*, The Verge, January 26, 2019. Available at https://www.theverge.com/2019/1/26/18197567/six-flags-illinois-biometric-information-privacy-act-facial-recognition. But *compare*, Shannon Liao, *Google wins dismissal of facial recognition lawsuit over biometric privacy act*, The Verge, December 29, 2018. *Available at* https://www.theverge.com/2018/12/29/18160432/google-facial-recognition-lawsuit-dismissal-illinois-privacy-act-snapchat-facebook.

73 SB 418. Available at https://www.capitol.hawaii.gov/session2019/bills/SB418_.HTM.

74 SD 341, SB 120. Available at https://malegislature.gov/Bills/191/S120

75 HB 1253, defeated in committee on February 5, 2019. Available at http://billstatus.ls.state.ms.us/2019/pdf/history/HB/HB1253.xml

76 SB 176. Available at https://www.nmlegis.gov/Sessions/19%20Regular/bills/senate/SB0176.pdf.

77 A 465. Available at https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A00465&term=0&Summary=Y&Text=Y.

78 HB 1485. Available at https://www.legis.nd.gov/assembly/66-2019/bill-index/bi1485.html.

79 SB 5376. Available at http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/Senate%20Bills/5376-S2.pdf.

80 Most state proposals also require that the company provide the report to the consumer "free of charge" but also have provisions preventing the abuse of such process. These provisions often limit the number of verified requests a consumer may submit within a 12-month period.

81 E.g. New Mexico SB 176, Massachusetts SB 120, and Hawaii SB 418.

82 Hawaii SB 418, above.

83 E.g. Massachusetts SB 120, Mississippi HB 1253, New Mexico SB 176 (Biometric information includes "an individual's physiological, biological, or behavioral characteristics, including... imagery of the… face.")

84 Arguing a person should have a privacy interest in his or her face is disingenuous and supports the proposition that these proposals are not focused on "privacy" but on corporate behavior. Members of the public recognize others' faces daily. A person's face appears on his or her

driver's license, his or her student identification, and any other number of places. People voluntarily upload countless volumes of photographs containing their faces to social media platforms daily. Whether people recognize others' faces or faces are used on driver's licenses, they purpose is for identification. Regulating what the private sector may, or may not do, with images of the face unnecessarily restricts from innovation very public information about people.

85 New Mexico SB 176.

86 New York A 465.

87 Washington SB 5376, above.

88 The full text of the language states that "The European Union recently updated its privacy law through the passage and implementation of the general data protection regulation, affording its residents the strongest privacy protections in the world. Washington residents deserve to enjoy the same level of robust privacy safeguards."

89 Tools include browsers with greater privacy protections, browser plug-ins, search engines that do not collect personal information, virtual private networks, privacy and do-no-track tools launched by Google and Facebook, and so on.

90 E.g. Muge Fazlioglu, *What FTC Enforcement Actions Teach Us About the Makings of Reasonable Privacy and Data Security Practices: A Follow-Up Study*, International Association of Privacy Professionals (IAPP), June 11, 2018. Available at https://iapp.org/news/a/what-ftc-enforcement-actions-teach-us-about-the-makings-of-reasonable-privacy-and-data-security-practices-a-follow-up-study/.

91 E.g. Waller, Spencer Weber, Jillian G. Brady, and R.J. Acosta, *Consumer Protection in the United States: An Overview*, available at http://www.luc.edu/media/lucedu/law/centers/antitrust/pdfs/publications/workingpapers/USConsumerProtectionFormatted.pdf (Waller, *Consumer Protection in the United States*)

92 *E.g.* Carter, Carolyn L. *Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes*, February 2009, National Consumer Law Center, Inc., available at https://www.nclc.org/images/pdf/car_sales/UDAP_Report_Feb09.pdf (Carter, *50-State Report*).

93 "Consumer Protection: An Overview of State Laws and Enforcement", 2010, Public Health Law Center at William Mitchell College of Law, available at http://www.publichealthlawcenter.org/sites/default/files/resources/phlc-fs-agconsumer-2010.pdf.

94 Carter, *50-State Report* at p. 12.

95 A common complaint is that privacy policies and terms of service are dense, escaping the understanding of non-lawyers. If states are serious about focusing on consumer protection, they could devote resources within the attorney general's office to reading through privacy policies and terms of service. The attorney general's office could use those resources to pursue companies violating those policies and provide consumers with meaningful translations from legalese.

96 Waller, *Consumer Protection in the United States* at 17.

97 *E.g.,* Carter, *50-State Report* pp. 7-10.

98 *See* "Consumer Protection: An Overview of State Laws and Enforcement", n.9, supra.

99 *Id.*

100 *Id.*, *see also* Carter, *50-State Report* at p. 6.

ALEC American Legislative Exchange Council

LIMITED GOVERNMENT • FREE MARKETS • FEDERALISM

American Legislative Exchange Council
2900 Crystal Drive, Suite 600
Arlington, VA 22202
Tel: 703.373.0933 • Fax: 703.373.0927 • www.alec.org

To learn more about how the American Legislative Exchange Council helps develop innovative solutions in partnership with lawmakers and business leaders, or to become a member, please visit www.alec.org.