State Attorneys General as Ideal Data Privacy Enforcers with the Passage of CCPA

Naomi King

The Legal and Political Importance of State Attorneys General

UCLA School of Law

I. Introduction

As a result of society's digital integration, large online companies track, obtain, and exploit user data for financial gain. This practice understandably raises privacy concerns with many Americans. However, large wealthy companies are a dauting opponent for the average American. In their busy day-to-day lives, most Americans don't have the resources to learn, much less do something about, the enormous amount of data these companies have collected on them. Meanwhile, companies like Google and Facebook make millions from such user data, often containing personal and intimate information. Whether consumers recognize it or not, these services are not free, instead they are paid for by users' personal information, which amounts to digital gold. In the absence of omnibus federal legislation in the privacy space, state attorneys general are a key protector of individual privacy rights. The Federal Trade Commission (FTC) is also responsible for federal privacy regulation, but the agency will not be a point of emphasis in this Note. This Note focuses the analysis on the role of state attorney general in data privacy and security enforcement, the limitations on available causes of action, and posits that state attorneys general continue to be the best option to regulate and enforce in the data privacy space given the passage of novel legislation like the California Consumer Privacy Act (CCPA).[1]

Data security and data privacy are two distinct concepts. Data security is one element of the broader idea of data privacy.[2] Data security refers to the protection of personal information held by an entity.[3] Data security is relevant to this Note as state attorneys general oversee data breach notification laws and are the key enforcers in this area. However, data security will not be the focus of this Note.

---

[1] California Consumer Privacy Act, Cal. Civ. Code §§1798.100-199 (West 2022).
[2] William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1141 (2019).
[3] *Id.*

Data privacy relates to the collection, use, and disclosure of personal data in addition to its secure storage.[4] This field has become more relevant as more and more of people's lives take place online. As a result, more of our personal information than ever before is stored on servers and vulnerable to leaks. Consumers have become increasingly aware of risks associated with the collection of their personal information. This Note will focus on data privacy concerns of consumers and the state attorneys general office's role in addressing these concerns. Data privacy is a rapidly evolving area of law, with new legislation being proposed and considered almost every legislative session in multiple states. Because we are in a rapidly evolving area of law, the legislation proposed has a huge impact on norms and what is considered compliant with current data privacy policies. Also, the norms consistently evolve based on emerging technologies.

II. Privacy as in the Public Interest and The Attorneys' General Responsibility

Privacy is a concept that has garnered growing media attention, and bipartisan support as politicians from both sides of the aisle increasingly demand that "big tech" respect the privacy of its users. Alan Westin, a preeminent privacy scholar, coined the term "informational privacy" as the power of "individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[5] This definition created the "privacy-control" paradigm that forms the basis of modern informational privacy law.[6] Privacy control focuses on an individual's ability to control and limit access to information about themselves.[7] Today, privacy is understood as a personal right to control the use of one's data.[8]

---

[4] *Id.*
[5] Henry Adams, *The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action,* 84 Mo. L. Rev. 1055, 1058 (2019).
[6] *Id.*
[7] *Id.*
[8] *Id.*

Controlling one's data concerns privacy because data often includes personal information, ranging widely from one's date of birth to their social security number to their religious beliefs.

With this understanding of privacy, we have a better grasp of what it means to retain one's privacy when engaging online. However, until recently, and still throughout most of the country, individuals' privacy rights are severely neglected. With Europe's General Data Protection Regulation (GDPR) and California's adoption of the California Consumer Privacy Act (CCPA), consumers' privacy issues are being addressed through the law. Meanwhile, private rights of action are still very rare. In the absence of such private causes of action, the responsibility of protecting those rights falls to the state attorneys general. It is, after all, the key responsibility of the state attorneys general to protect the public interest.[9] Today, most Americans would agree that it is in the public interest to protect an individual's privacy.

III. History of State Attorneys General Involvement in Data Privacy

State attorneys general have been at the forefront of privacy regulation.[10] In the mid-to-late twentieth century, state attorneys general pursued consumer protection, which has expanded to include privacy and data concerns.[11] States adopted unfair and deceptive trade acts and practices laws (UDAP laws) which ban deceptive commercial acts and practices and unfair trade acts and practices.[12] UDAP laws are attorneys general's key tool in their privacy-related enforcement efforts.[13] Attorneys general offices began focusing on privacy issues in the 1990s.[14] During that period, enforcement efforts focused on telemarketing, spam, spyware, and the lack of

[9] Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747, 753 (2016).
[10] *Id.* at 754.
[11] *Id.* at 753.
[12] *Id.* at 754.
[13] *Id.* at 750.
[14] *Id.* at 754.

privacy policies.[15] Today, the data privacy mantle includes protecting users from data breaches, identity theft, and regulating privacy policies and private browsing.[16] Leading states in the privacy space, such as California, have their own subdivision dedicated to privacy within the consumer protection division of the attorney general's office.

Since their involvement in the space, attorneys general have developed privacy law through legislation, education, and enforcement.[17] Attorneys general propose and endorse state consumer privacy and data security laws.[18] They educate the public through the issuance of best practice guides.[19] These guides provide companies with notice regarding what attorneys general offices consider to be unfair and deceptive practices, and more generally these guides explain a state attorney general's understanding of current privacy law.[20] Briefly surveying the history of attorney general involvement in data privacy reveals that in many ways, the states have been instrumental in developing privacy law.

IV. Why the State Attorney General Should be Charged with Privacy Enforcement

Various state attorneys general have already played an important role in responding to privacy issues as a means of pursuing the public interest. The state attorneys general office is ideally positioned to enforce such claims. One of the most compelling reasons for the role of the state attorneys general is that private claimants often run into standing issues when pursuing their privacy rights.[21] The four privacy torts: intrusion on seclusion, public disclosure of private fact, false light, and misappropriation of image, have been interpreted narrowly.[22] As a result, they are

---

[15] *Id.*
[16] *Internet and Privacy*, National Association of Attorneys General, https://www.consumerresources.org/consumer-topics/internet-and-privacy/#toggle-id-8-closed.
[17] Citron at 750.
[18] *Id.* at 758.
[19] *Id.* at 760.
[20] *Id.*
[21] *Id.* at 798.
[22] *Id.*

not feasible pathways for recovery in the data privacy space. To satisfy standing requirements, the presence of injury-in-fact is crucial in privacy litigation.[23] The Supreme Court has interpreted injury-in-fact to mean that the injury must be: (1) "an invasion of a legally protected interest, (2) that is concrete and particularized," and (3) that is "actual or imminent, not conjectural or hypothetical."[24] Overall, the Supreme Court has been skeptical of data privacy harms.[25] The law has been slow to acknowledge non-physical harms, and that same hesitancy is seen in the realm of privacy law. The requirement of concreteness means that an injury must be "real and not abstract."[26] In data privacy cases, the courts have been hesitant to interpret an infringement of data privacy as a real and not an abstract legally protected interest. Therefore, it remains to be seen whether the protection of personal data is a legally conferred right.[27] In the interim, these standing issues preclude private claimants from seeking redress of infringements of their data privacy.

Further, an individual user faces overwhelming resource asymmetry when going up against large online service providers. The David versus Goliath analogy is fitting when imagining a single plaintiff with limited resources seeking redress against huge tech companies' armies of top-tier lawyers with almost unlimited resources. There are also systematic disadvantages that individuals face. For example, consumers begin with a disadvantage because they are required to share personal information to access online services without understanding what privacy rights are given up in exchange.[28] Thus, there is huge informational asymmetry as

---

[23] Juan Olano, *The Struggle to Define Privacy Rights and Liabilities in A Digital World and the Unfortunate Role of Constitutional Standing*, 72 U. Miami L. Rev. 1025, 1040 (2018).
[24] Olano at 1040 (quoting *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016)) (quoting *Lujan*, 504 U.S. at 560)).
[25] Anupam Chander, Margot E. Kaminski, and William McGeveran, *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733, 1762 (2021).
[26] Olano at 1043.
[27] *Id*. at 1042.
[28] FORBRUKARRÅDET, DECEIVED BY DESIGN 6 (June 27, 2018), https://www.dwt.com/-/media/files/blogs/privacy-and-security-blog/2020/12/deceived-by-design.pdf.

consumers are often blissfully unaware of the privacy rights they give up to access "free" online sites and services. For example, many consumers go unaware that as they use an application, their minute-by-minute location is being tracked and could be sold to a third party who monetizes this data. A Pew Research poll found that 74% of Facebook users were not aware that the site lists their traits and interests for advertisers.[29] Thus, there is information asymmetry as most consumers are unaware of what rights they surrender when using online services.

The state attorneys general office is better positioned to respond to privacy issues than federal agencies. First, the FTC faces a lack of resources. The FTC's ability to enforce privacy norms with Section 5 is severely lacking due to the agency's limited capacity, expanding regulatory responsibilities, and general approach to enforcement.[30] In terms of resources, the Division of Privacy and Identity Protection's fifty-two employees clearly does not provide the FTC with the capacity to respond effectively to all incidents.[31] Conversely, states are in a better position because they can focus on a more limited constituency base and tailor their response to capture breaches resulting from new technologies. Further, the FTC does not engage in formal rulemaking to regulate data practices under its Section 5 authority.[32] To engage in rulemaking, the FTC must meet burdensome standards, and instead the agency relies on enforcement as its primary way to regulate corporate practices.[33] Conversely, state attorneys general have frequently lobbied state legislatures for specific laws. State regulation has taken on two important forms: pioneering state efforts where states identify areas lacking regulation or create

---

[29] John Gramlich, *10 Facts About Americans and Facebook*, PEW RES. CTR. (June 1, 2021), https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/.
[30] Henry Adams, *The Federalist Regulation of Privacy: The Happy Incidents of State Regulatory Activity and Costs of Preemptive Federal Action*, 84 Mo. L. Rev. 1055, 1066 (2019).
[31] *Id.*
[32] Elysa M. Dishman, *Settling Data Protection Law: Multistate Actions and National Policymaking*, 72 Ala. L. Rev. 839, 842 (2021).
[33] *Id.*

new regulatory methods, and gap-filling where the states enforce existing federal laws.[34] Thus, state attorneys general also complement federal enforcement in the privacy space.

Relatedly, the enforcement goals of the FTC and the state attorneys general often diverge. State enforcers can be more consumer-focused as compared to their federal counterparts. Consider the enforcement action in which state and federal authorities investigated Google and the advertising firm PointRoll. While Google's privacy policy promised that it respected the privacy setting of its users, it was revealed that Google changed users' settings and placed third-party cookies on Safari users' browsers whose settings signaled they did not wish to be tracked.[35] The FTC invited a multistate group composed of thirty-nine attorneys general to join their consent decree.[36] However, the multistate group declined because they had a different goal in mind in their investigation. The multistate group sought injunctive relief.[37] Because the FTC's consent decree did not place a prohibition on Google's future behavior, the multistate group did not think it went far enough.[38] The state approach relies on these settlements to convey data standards to corporations by mandating that these corporations undergo structural reforms as part of any settlement negotiation.[39] These structural reforms serve as models to all actors in the data privacy space indicating what is now considered compliance, given that norms constantly evolve.

State attorneys general also have the advantage of being able to pursue multistate advocacy which often result in large and robust multistate settlements. Multistate advocacy is a powerful tool because it allows state attorneys general offices to pool resources. Such pooling of resources allows for a fairer fight, as the states' cooperation creates more opportunity to face the

---

[34] Adams at 1069.
[35] Citron at 769.
[36] *Id.* at 770.
[37] *Id.*
[38] *Id.*
[39] Dishman at 844.

huge tech companies' armies of lawyers. A core group of states have emerged as leaders in the data privacy space: California, Connecticut, Illinois, Indiana, Maryland, Massachusetts, New Jersey, New York, North Carolina, Ohio, Pennsylvania, Texas, Vermont and Washington.[40] These state attorneys general offices spearhead multistate investigations, apart from their active individual enforcement actions.[41] The state attorneys general acting in concert can obtain agreements in these settlements that individual plaintiffs, or a lone federal agency, could not obtain. Take, for example, the Google Street View incident that was led by Connecticut Attorney General George Jepsen. In the Google Street View incident, the negotiated settlement went beyond monetary damages and included an educational campaign run by Google to educate the public about privacy issues such as learning how to encrypt their Wi-Fi.[42] It also mandated that Google establish a privacy program and training for their employees.[43] The settlement went far beyond monetary damages. These settlements are a key tool that the attorneys general use to shape corporate practices in the data privacy space and create data privacy policy.[44] These multistate settlements have been a primary way in which states have innovated through the implementation of structural reforms.[45]

State attorneys general offices, acting together, also increase their bargaining position vis-à-vis the company with whom they are in settlement negotiations.[46] In the tobacco litigation

---

[40] Citron at 755.
[41] *Id.*
[42] Press Release, Office of the Att'y Gen. of CT., Attorney General Announces $7 Million Multistate Settlement With Google Over Street View Collection of WiFi Data (March 12, 2013), https://portal.ct.gov/AG/Press-Releases-Archived/2013-Press-Releases/Attorney-General-Announces-7-Million-Multistate-Settlement-With-Google-Over-Street-View-Collection-o.
[43] David Streitfeld, *Google Concedes That Drive-By Prying Violated Privacy*, N.Y. Times, (March 12, 2013), https://www.nytimes.com/2013/03/13/technology/google-pays-fine-over-street-view-privacy-breach.html.
[44] Dishman at 844.
[45] *Id.*
[46] Donald G. Gifford, *Impersonating the Legislature: State Attorneys General and Parens Patriae Product Litigation*, 49 B.C. L. Rev. 913, 944 (2008).

in which the state attorneys general took on "Big Tobacco" to recover smoking-related costs, more than forty states negotiated as a single block.[47] The scope of interstate cooperation was unprecedented, and the size of the eventual settlement was likewise groundbreaking.[48] Beyond the impressive settlements, interstate cooperation affects public opinion. Prior to the tobacco litigation, the tobacco industry had never lost a case, in part due to juror sentiment.[49] After the litigation concluded, the industry suffered several trial defeats.[50] Thus there was a marked change in public sentiment towards "Big Tobacco." In a similar way, state attorneys general can shift public sentiment against "Big Tech" in data privacy realm. The tobacco litigation has served as a model of successful bipartisan multistate settlement. In the major data privacy cases, there are often upwards of 20 states involved in these settlement negotiations, replicating the increased bargaining power of the states that has proved successful.

Further, state attorneys general offices are closest to the average American, who can reach their state attorneys general office much quicker than they could reach a federal agency that serves the entire country. Federal agencies are known for their bureaucracy, and while states do not completely escape administrative hurdles, they are typically smaller, more accessible, and serve a more manageable constituency. Moreover, the state approach to data privacy allows for addressing different concerns since issues that residents of California consider to be important may very well be distinct from issues that Florida residents consider to be important. In this way, a more diverse set of privacy claims can be addressed.

---

[47] *Id.* at 944.
[48] Richard P. Ieyoub and Theodore Eisenberg, *State Attorney General Actions, the Tobacco Litigation, and the Doctrine of Parens Patriae*, 74 Tul. L. Rev. 1859, 1860 (2000).
[49] *Id.*
[50] *Id.* at 1861.

Attorney general activism can also create policy change in an era of gridlock in federal institutions.[51] Justice Louis Brandeis commented that "It is one of the happy incidents of the federal system that a single courageous state may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the country."[52] States serve as laboratories of democracy in the data privacy space as states like California pave the way through adopting novel legislation that protects individual privacy rights. Most notably, the CCPA.

State attorneys general are also nimble enough to respond to novel issues. A good example can be found in the state response to data brokers. There has been a growing phenomenon where data brokers collect personal information and sell it to companies, government agencies, and others. This area is mostly unregulated, resulting in increased risk of infringements on individual privacy rights. The California legislature passed a law that requires data brokers to register with the attorneys general office and which requires users to have the option to opt out of the sale of their personal information.[53] However, there is still stronger regulation which is needed to restrict the industry exploiting personal data.

Moreover, state attorneys general have even led the charge in lobbying for new legislation. For example, in 2003, the California Online Privacy Protection Act was proposed by the California Attorney General.[54] States have been known to encourage state legislatures to promulgate data privacy legislation.[55] Data breach notification laws serve as another illustrative

---

[51] Paul Nolette, *State Attorneys General are More and More Powerful. Is that a Problem?* The Washington Post, (March 5, 2015) https://www.washingtonpost.com/news/monkey-cage/wp/2015/03/05/state-attorneys-general-are-more-and-more-powerful-is-that-a-problem/?variant=15bc93f5a1ccbb65.
[52] *Id.*
[53] *Data Brokers*, Electronic Privacy Information Center, https://epic.org/issues/consumer-privacy/data-brokers/ [hereinafter: Epic].
[54] Citron at 764.
[55] Dishman at 857.

example. Data breach notification laws require covered entities to notify the residents of a state to inform them that their unencrypted personal information was acquired by an unauthorized entity. State attorneys general lobbied their state legislatures to adopt data breach notification laws.[56] Now, every state in the country has a form of such law.[57]

Further, regulating in the face of uncertainty requires flexibility. With ever increasing technological advancements and new uses for user data, the need for flexibility in the data privacy law is apparent. Thus, the structure of the attorneys general office is more conducive to responding to such change as compared to a bureaucratic federal agency.

V. Rise of Privacy Concerns

Privacy concerns have increased with the awareness of national scandals like Google's Street View incident. In May 2010, Google first disclosed that it had collected and stored "payload data" from unsecured wi-fi networks while Google's Street View cars drove around cities all throughout the world collecting images for Google's mapping service.[58] The "payload data" included the content of users' Internet communications, including "email, medical and financial records, passwords" among other personal information.[59] From 2008 to May 2010, Google equipped these cars with antennae and open-source software that collected information from unsecured wireless networks.[60] Initially, Google indicated that the collection of this data

---

[56] *Id.*
[57] *Id.*
[58] Hibah Yousuf, *38 States Press Google on Personal Data*, CNN Money (July 22, 2010), https://money.cnn.com/2010/07/22/technology/Google_street_view_privacy/index.htm?section=money_topstories&utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+rss%2Fmoney_topstories+%28Top+Stories%29.
[59] Streitfeld, *supra* note 43.
[60] Press Release, Office of the Att'y Gen. of WA, Google to Pay $7 Million in Multistate Settlement Over Street View (March 12, 2013), https://www.atg.wa.gov/news/news-releases/google-pay-7-million-multistate-settlement-over-street-view.

was a mistake.[61] However, later allegations surfaced that members of the Google team did in fact know about the interception of the payload data.[62] Upon the disclosure of the Google Street View incident, the public was outraged and public concern over privacy issues heightened.

Another example of a concerning practice that infringes on individual privacy rights is the use of dark patterns. The term was coined by user experience researcher Harry Brignull.[63] Dark patterns include "… features of interface design created to trick users into doing things that they might not want to do, but which benefit the business in question."[64] Specifically, digital service-providers use dark patterns to nudge users towards privacy intrusive options.[65] Examples of dark patterns include "aspects of design such as the placement and color of interfaces, how text is worded."[66] Another example is the preselection of privacy intrusive options through default settings. In 2018, a report found that both Facebook and Google, two of the largest digital service providers, had default settings preselected to the least privacy friendly option.[67] The combination of privacy intrusive settings and confusing wording obscuring what opting in to a setting actually means, constitutes a dark pattern.[68] Dark patterns are controversial because these schemes trick users into making choices that are not in their best interest, and take away a user's agency.[69] Further, there is a huge information asymmetry issue, as most users are not aware of the privacy risks associated with their use of an online service.[70]

---

[61] *Creating Stronger Privacy Controls Inside Google*, Google Policy Blog (October 22, 2010), https://publicpolicy.googleblog.com/2010/10/creating-stronger-privacy-controls.html
[62] David Kravets, *An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle*, WIRED (May 2, 2012), https://www.wired.com/2012/05/google-wifi-fcc-investigation/.
[63] FORBRUKARRÅDET, *supra* note 28 at 7.
[64] *Id.*
[65] *Id.* at 3.
[66] *Id.* at 6.
[67] *Id.* at 15.
[68] *Id.* at 18.
[69] *Id.*
[70] *Id.* at 6.

Selling the personal data of users has become big business.[71] Apart from selling user data to advertisers, an entire industry known as data brokers has sprung up around the idea of selling user data. Data brokers buy, aggregate, disclose, and sell billions of data elements on Americans.[72] One issue with data brokerage firms is that the definition of what constitutes such a firm is not consistent.[73] While California passed a law targeted at data brokerage firms that requires them to register with the state attorney general, the definition of who qualifies as such a firm is very narrow, thus leaving large numbers of firms who buy and sell user data, yet are exempted from complying with those laws.[74] Thus, data brokers remain under-regulated.

Privacy concerns increase as companies' misuse of user data come to light. One such incident was the Cambridge Analytica data privacy scandal. The research firm collected user data without their consent from individual Facebook accounts, in a practice known as "data harvesting." Facebook revealed that data on 87 million people was improperly shared with the firm.[75] Cambridge Analytica then used that data to allegedly manipulate U.S. voters in the 2016 election.[76] In response to the Cambridge Analytica scandal, Americans distrust of "big tech" soared to new heights. The scandal provided support for the activists who led the charge on the creation of a ballot measure that ultimately resulted in the CCPA.[77] One of the two leading activists remarked, "After the Cambridge Analytica scandal, all we had to say was 'data

---

[71] Alexandria J. Saquella, *Personal Data Vulnerability: Constitutional Issues with the California Consumer Privacy Act*, 60 Jurimetrics J. 215, 217 (2020).
[72] Epic, *supra* note 50.
[73] Justin Sherman, *Data Brokers and Sensitive Data on U.S. Individuals*, 2 https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf.
[74] *Id.*
[75] Sara Salinas, *Facebook Says the Number of Users Affected by Cambridge Analytica Data Leak is 87 Million*, CNBC (Apr. 4, 2018), https://www.cnbc.com/2018/04/04/facebook-updates-the-number-of-users-impacted-by-cambridge-analytica-leak-to-87-million-.html.
[76] Chander at 1783.
[77] Nicholas Confessore, *The Unlikely Activists Who Took on Silicon Valley—and Won*, N.Y. Times Mag. (Aug. 14, 2018), https://www.nytimes.com/2018/08/14magazine/facebook-google-privacy-data.html.

privacy."[78] In the preamble to the CCPA, the California legislature indicated this incident influenced the CCPA's passage.[79]

VI. Available Doctrines and Limitations

As noted before, UDAP laws are central to state attorneys general enforcement powers in the privacy space. One benefit of these laws is that they tend to be broad and fluid, which gives state attorneys general the flexibility to address novel privacy issues.[80] Moreover, interpretation under these acts continues to evolve, so that what was once considered compliance with best practice can now be interpreted as failure to comply and vulnerable to enforcement.[81] Attorney Generals are also seeking to expand their UDAP authority on specific privacy issues.[82] Consider Maryland, where the Attorney General petitioned the state legislature to increase his UDAP authority to allow him to bring lawsuits under the federal Children's Online Privacy Protection Act (COPPA).[83] However, UDAP laws also have limitations. Importantly, they often come with ranges for damages which are problematic for state attorneys general offices. For example, a statute might stipulate that any violation is $1,000 to $10,000 per violation. If there is a range, then judges have discretion over the amount of damages. Often, a judge may be inclined to reward the lower amount. This results in companies having to pay on the lower side of the range. Even if the case doesn't go to trial, and they most often do not, companies can offer lower settlement amounts knowing that if the case went to trial the damages amount would be relatively low. This is especially true for the huge social media companies with the most market

[78] Confessore, *supra* note 74.
[79] Chander at 1783.
[80] Divonne Smoyer, *The Growing Reach of State Attorneys General Over Data Privacy and Security Breach Incidents*, in RECENT TRENDS IN PRIVACY AND DATA SECURITY 173, 3 (2013).
[81] *Id.*
[82] *Id.*
[83] *Id.*

share who have significant funds to pay for these settlements. If the statute delineated a concrete set of damages, companies would likely tighten their privacy protocols.[84]

State attorneys general also have the unique authority to bring *parens patriae* actions on behalf of the citizens in their state. The *parens patriae* authority is uniquely reserved to the states. The doctrine has a long history in American jurisprudence and is rooted in common law. *Parens Patriae* allows a state to "bring an action on behalf of its citizens in order to protect its quasi-sovereign interest in the health, comfort, and welfare of its citizens."[85] States often bring these actions in the area of data protection under their general consumer protection statutes.[86]

Additionally, federal regulations relating to healthcare, children's online activity, and credit reporting agencies are enforceable by state authorities.[87] The federal regulations that are available are limited to specific subject-areas: data security for covered entities in healthcare through the Health Insurance Portability and Accountability Act (HIPPA), the privacy provisions of the Gramm-Leach-Bliley Financial Modernization Act that regulate the financial services sector, and the regulation of data collected on minors through COPPA. While state attorneys general have the authority to prosecute under federal privacy statutes in the privacy space, the regulations are quite narrow and leave large swaths of privacy issues unaddressed.

State attorneys general have also been important enforcers in the data security space, especially when companies suffer data breaches which potentially compromise user information. Enforcement efforts are crucial in this area as companies continue to underinvest in security.[88] California was the first state to enact a breach notification statute in 2003.[89] California's state

[84] Telephone interview with Tim Murphy, Senior Deputy Attorney General, Pennsylvania Office of Attorney General (March 23, 2022).
[85] Jack Ratliff, *Parens Patriae: An Overview*, 74 Tul. L. Rev. 1847, 1847 (2000)
[86] Dishman at 856.
[87] Citron at 778.
[88] McGeveran at 1138.
[89] *Id.* at 1152.

attorneys general office posts past data breach notifications on its website. The office also publishes a report which includes recommendations of best practices for companies to follow as a means of clarifying the data breach statute.[90]

As discussed previously, state attorneys general rely on the laws passed by the legislatures. This is a significant way through which the institution of the attorney general can enforce privacy issues as they emerge. These laws vary state-by-state. In California, the best example of this system working is the passage of the CCPA.

VII. CCPA Expanding State AG Enforcement in Data Privacy

The passage of the CCPA, codified at Cal. Civ. Code §1798.100 *et seq*, serves as a model of states enacting legislation that allows state attorneys general to get involved in data privacy in a more robust way. As one of the activists who is responsible for the CCPA's eventual consideration and passage put it, "Under [the CCPA], the attorney general of California will become the chief privacy officer of the United States of America."[91] Prior to the CCPA, no federal or state statute imposed privacy protections across all sectors and technologies.[92] Thus, the CCPA is remarkable for its transcendence of sectoral framework that has characterized the data privacy space for decades.

Before considering the substance and the potential impact of the CCPA, it is worthwhile to note the illuminating way in which the legislation came about. In California, citizens have the power to introduce legislation through ballot initiatives.[93] So long as a California citizen receives the requisite number of signatures on a petition, they can secure a statewide vote on their

---

[90] *Id.* at 1157.
[91] Confessore, *supra* note 74.
[92] Chander at 1738
[93] Courtney M. Bowman and Kristen J. Matthews, *The California Consumer Privacy Act of 2018*, (July 13, 2018) https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer-privacy-act-of-2018/.

initiative.[94] The activists who were behind the ballot initiative collected nearly twice the required minimum, and the initiative was slated to appear on the ballot in the November 2018 general election.[95] Lawmakers, realizing that the ballot initiative was likely to be successful, struck a deal with the activists who promised to remove the ballot measure in exchange for the passage of the CCPA.[96] The story of the CCPA's passage is illuminating because it shows that data privacy concerns are at the forefront of consumer concern. Ordinary people led the charge to get the CCPA passed. The passage illuminates the fact that everyday people are growing increasingly concerned that their data privacy rights are being infringed upon.

The CCPA is significant for many reasons, one of which is for its novel recognition of distinct rights. Notably, the CCPA provides California residents with notice rights, and places an emphasis on the right to have notice.[97] Companies are required to disclose the purpose of processing data, categories of information gathered, and the existence of individual rights with respect to the data.[98] Here the state attorneys general serve an important role as he or she promulgates regulations surrounding these disclosures. Thus, the state attorney general has the ability to clarify the law and shape it through regulations. For example, the Attorney General of California promulgated a regulation indicating these notices must be "designed and presented in a way that is easy to read and understandable to consumers."[99] The CCPA also provides users with access rights.[100] The CCPA creates a right for consumers to request the specific piece of personal information that a business has collected.[101] CCPA's access rights are a notable

---

[94] *Id.*
[95] Confessore, *supra* note 74.
[96] *Id.*
[97] Chander at 1751.
[98] *Id.*
[99] *Id.* at 1752 (citing Cal. Code Regs. Tit. 11, §999.305(2)).
[100] *Id.* at 1752.
[101] *Id.*

improvement from previous U.S. law, which provided consumers with very limited rights of access, for example, to credit scoring information.[102] There is also a right to opt out and refuse a business from handling one's data in certain ways.[103] The CCPA also includes a limited right to deletion that applies only to businesses that collect data directly from a user.[104]

As discussed above, the CCPA is remarkable for its substance. The legislation also marks a notable shift from existing privacy law for several reasons. First, the CCPA is notable for its form. It takes a comprehensive approach to regulating the use of user data. Data privacy laws in the past have been largely industry-specific and narrow. The entire United States' framework has been characterized as fragmented: "[t]he framework consists of hundreds of state and federal statutes, regulations, binding guidelines, and court created rules" that concern data security and privacy.[105] There are federal laws that govern specific industries like health care and the financial sector. However, even within an industry that is regulated, the particular law may not govern the entirety of data privacy within that industry.[106] In contrast, the CCPA governs all online service providers who meet specific qualifications to be covered by the law. In effect, the CCPA is the first consequential non-industry-specific law that governs in the privacy space.

Second, the legislation takes a broad definition of personal information that exceeds most existing privacy laws in the US.[107] Historically, narrow definitions of personal information have stubbed the influence of privacy laws.[108] In the CCPA, personal information is defined as "capable of being associated with, or could reasonably be linked, directly or indirectly, with a

---

[102] *Id.*
[103] *Id.* at 1753 (citing Cal. Civ. Code § 1798.120(a)).
[104] *Id.* at 1754 (citing Cal. Civ. Code § 1798.105 (2018)).
[105] Carol Li, *A Repeated Call for Omnibus Federal Cybersecurity Law*, 94 Notre Dame L. Rev. 2211, 2213 (2019) Quoting Jeff Kosseff, Cybersecurity Law 1 (2017) at xxi.
[106] *Id*. at 2214.
[107] Chander at 1749.
[108] *Id.*

particular consumer or household."[109] The statute then provides a comprehensive list of examples of personal information, ranging widely from real name, email address, social security number, driver's license number, biometric information, and geolocation data.[110]

Moreover, the CCPA tackles new issues head-on. For example, it regulates data brokers directly, an industry that has a large impact on individual privacy rights.[111]

The CCPA is likely to have what David Vogel coined "the California effect," when companies have a strong incentive to follow the regulatory standards of powerful states.[112] Vogel coined the term describing how one jurisdiction pushes other jurisdictions to improve their own laws.[113] In this way, the CCPA will likely have a significant effect on other states. The so-called California effect is evident in the data security space through the development of data breach notification laws. California was the first state to enact a data breach notification law and other states quickly followed with their own laws. Data notification laws require companies which experience a qualifying data breach to notify users whose personal information potentially was compromised by the breach.[114] Today, all fifty states have data breach notification laws.[115] In fact, the California effect in the privacy space is becoming apparent as states have already begun proposing and passing their own comprehensive data privacy laws.[116]

The effect of the CCPA and amendment is that it will likely continue to influence other states to adopt similar legislation. In 2018 and 2019, seventeen states and Puerto Rico considered comprehensive data privacy laws resembling the CCPA.[117] Virginia followed California making

---

[109] Chander at 1749 citing Cal. Civ. Code §1798.140(o)(1).
[110] Cal. Civ. Code § 1798.140(o)(1)(A),(E),(G).
[111] Chander at 1749-1750.
[112] *Id.* at 1743.
[113] *Id.*
[114] *Id.* at 1785
[115] *Id.* at 1786.
[116] *Id.* at 1763.
[117] *Id.* at 1771.

it the second state to pass a comprehensive data privacy bill.[118] Examining another such piece of legislation in Connecticut shows similarities to the CCPA: the same definition of personal information and covered business, and granting access rights, a right to deletion, and a right to opt out of the sale of one's data.[119] California has exerted itself as an expert on data privacy law, due to its pioneering lawmaking in data privacy and Silicon Valley's presence in the state.[120] Moreover, the CCPA will have an impact because of California's outsized market share. Many companies do business in California, thus they have likely been forced to comply with the new law. If these businesses do not do business in California, then they likely engage with California consumers and thus would have to be compliant with the CCPA. Thus, many companies already comply with the CCPA and are readily able to comply with CCPA-like requirements in other states.[121] Because other states are copying California's model, the state attorneys general in those jurisdictions are likely to expand their enforcement abilities through this type of legislation. Given the rapid adoption of similar legislation in other states, the state approach appears to be creating a national standard for privacy. As a result, there becomes less of an obvious need for a federal omnibus privacy law.

California has continued to lead the way in this space, and it has gone farther in pursing privacy rights. California voters approved the California Privacy Rights Act (CPRA) in November 2020, which amends the CCPA and takes effect on January 1, 2023. Among the most significant change is the creation of the California Privacy Protection Agency (CPPA) which has the authority to create data privacy regulations.[122] The CPPA is charged with "full administrative

---

[118] Rebecca Klar, *Virginia Governor Signs Comprehensive Data Privacy Law*, The Hill (Mar. 2, 2021), https://thehill.com/policy/technology/541290-virginia-governor-signs-comprehensive-data-privacy-law/.
[119] Chander at 1772.
[120] *Id.* at 1784.
[121] *Id.* at 1764.
[122] Andraya Flor, *The Impact of Schrems II: Next Steps for U.S. Data Privacy Law*, 96 Notre Dame L. Rev. 2035, 2042 (2021).

power, authority, and jurisdiction to implement and enforce" the CCPA.[123] California Attorney General Xavier Becerra said, "The [CPPRA] marks a historic new chapter in data privacy by establishing the first agency in the country dedicated to protecting forty million Californians' fundamental privacy rights."[124] The CPRA expressly provides that "the agency may not limit the authority of the Attorney General to enforce this title."[125] While the agency will be able to bring enforcement actions related to either the CCPA or CPRA before an administrative law judge, the attorney general still maintains civil enforcement authority over both laws.[126] Ashkan Soltani, who worked on both the CCPA and the CPRA, will head the agency as its first executive director.[127] The agency will also be governed by a five-person board comprised of experts in the data privacy space. The fact that experts will be dedicated to consumer rights is monumental, as one hurdle in privacy law is that even those who care and desire to effect change in this area are limited by their lack of technical knowledge. The agency is promising because it is the first of its kind in being solely dedicated to data privacy, without other enforcement obligations.[128] Allowing the agency to focus exclusively on data privacy will likely result in robust promulgation of data privacy norms and best practices.

---

[123] Office of Governor Gavin Newsom, California Officials Announce California Privacy Protection Agency Board Appointments, Office of Governor Gavin Newsom (Mar. 17, 2021), https://www.gov.ca.gov/2021/03/17/california-officials-announce-california-privacy-protection-agency-board-appointments/.
[124] *Id.*
[125] Cal. Civ. Code § 1798.199.90 (West).
[126] *Supra* note 119.
[127] Press Release, Office of the California Governor, Ashkan Soltani Selected as California Privacy Protection Agency Executive Director (October 4, 2021), https://cppa.ca.gov/announcements/index.html#20211005.
[128] Chander at 1759-1760.

Just as important is the universal opt out created in the CPRA. The CCPA already allowed consumers to opt-out of the sale of their personal information.[129] CPRA went further by allowing consumers to opt-out of the use and disclosure of their personal information.[130]

The CPRA also takes aim at dark patterns. The CPRA makes explicit that "consent" obtained through the use of dark patterns does not constitute actual consent.[131] The definition of "consent" provided in the statute explicitly includes, "agreement obtained through the use of dark patterns does not constitute consent."[132] Further, the CPRA directs regulations to ensure that "any link to a web page or its supporting content that allows the consumer to consent to opt in does not make use of any dark patterns."[133]

Criticisms

The CCPA is not without its critics. While the CCPA and the CPRA undoubtedly mark a progression in the data privacy field, some are skeptical about the legislations' effect based on how it will be promulgated in practice. To date, there has been no litigation surrounding the CCPA. While it's recent adoption may explain why there has not been litigation, there is still a significant concern that the implementation of the law will fall below what the activists imagined the CCPA's effect would be.

Some critics argue that the CCPA does not go far enough because it does not create a private right of action, apart from in the limited case of certain data security breaches.[134] Thus, only state

---

[129] Katelyn Ringrose, *New Categories, New Rights: The CPRA's opt-out provision for sensitive data*, IAPP (Feb. 8, 2021), https://iapp.org/news/a/new-categories-new-rights-the-cpras-opt-out-provision-for-sensitive-data/.
[130] *Id.*
[131] Christopher W. Savage, "Dark Patterns" Make Their Appearance in California's New Privacy Law, 26 No. 2 Cyberspace Lawyer NL 5.
[132] Cal. Civ. Code §1798.140(h).
[133] Cal. Civ. Code §1798.185(a)(20)(C)(iii).
[134] Chander at 1759 n.166 ("The CCPA does, however, authorize private lawsuits for a narrow set of claims related to data security breaches.").

attorneys general have the authority to enforce most of the provisions of the law.[135] However, as discussed previously, state attorneys general may be best positioned to enforce individual privacy rights, even as compared to individuals themselves. Further, critics point out that the CCPA does not change the default setting on data processing in California.[136] It also does not tackle algorithmic accountability.[137] While the CCPA can go further, the adoption of the CPRA and the establishment of the CPPA, prove that there is advancement in this area of the law and more to come as the state attorneys general enforces the CCPA.

Critics may point out that there are serious limitations to the CCPA that can potentially curtail its adaption in other states. First, it is limited by the regulated entities to whom it applies. The CCPA only applies to businesses that meet a complex set of overlapping requirements.[138] Nonprofits and governments, for example, are excluded. Second, critics have raised the possibility that the CCPA may not survive a commerce clause challenge.[139] The argument would allege that the CCPA poses an excessive burden on interstate commerce.[140] Ultimately, a court will need to decide whether California's interest in protecting the privacy rights of its residents justify the costs imposed on businesses operating in interstate commerce.[141] However, the commerce clause challenge is less concerning to privacy advocates as the CCPA does not appear to facially discriminate against interstate commerce.[142] Thus, any commerce clause challenge is unlikely to pose a serious threat to the CCPA's promulgation.

---

[135] Chander at 1759.
[136] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. Rev. 1687, 1712 (2020).
[137] *Id.* at 1712.
[138] *Id.* at 1758.
[139] *Id.* at 1794.
[140] *Id.* at 1796.
[141] *Id.*
[142] *Id.*

A more concerning criticism regarding the CCPA's potential effect on a nationwide scale is that the CCPA could also be diminished if Congress chooses to pursue an omnibus federal privacy law that could result in preemption of all or some of the CPPA.[143] State laws may be preempted when compliance with both state and federal laws is impossible.[144] If Congress were to enact a federal privacy statute with an express preemption clause, the CCPA would be rendered moot. There are indications that Congress would not pass such a law, as House Speaker Nancy Pelosi vowed not to support any federal privacy law that affords less protection of individual privacy rights than the CCPA or that preempts state law.[145] Any federal law that is passed should provide a nationwide floor, allowing states to adopt more protective laws.[146] This way, the federal law does not prevent state attorneys general offices from being the key enforcers in this area. In fact, most federal laws do serve as regulatory floors.[147] Thus, it is more likely that any federal law that is passed in the data privacy space will also serve as a floor rather than a ceiling.

Another serious limitation on the attorney generals' enforcement ability is funding. There is a lack of sufficient funding for privacy divisions within state attorneys general offices across the country. As discussed previously, state attorneys general offices who go against big tech's armies of lawyers are under-resourced and thus disadvantaged. While there might be laws on the books, they may not have the intended effect unless these offices are properly funded. The CPPA, the agency created through the CPRA, is first of its kind. Nevertheless, with consistent

---

[143] *Id.* at 1797
[144] *Id.*
[145] *Id.* at 1797. Citing Darius Tahir, *Pelosi Puts Privacy Marker Down*, POLITICO (Apr. 15, 2019), https://www.politico.com/newsletters/morning-ehealth/2019/04/15/pelosi-puts-privacy-marker-down-424986 [https://perma.cc/GJ39-7J9J].
[146] *Id.* at 1797.
[147] *Id.*

funding earmarked and an established structure, the CPPA has potential to change the landscape of data privacy enforcement in California.

Others criticize state attorneys generals' multistate settlements. Critics point to the fact that these settlements are negotiated behind closed doors and with little involvement from other stakeholders.[148] Still others argue that these settlements don't go far enough. For example, after the Google Street View scandal was uncovered and investigated, nine states criticized the eventual settlement as not going far enough because it did not offer compensation for the victims whose data was captured.[149] Further, the settlement amount that resulted from the multistate investigation into Google was $7 million. When considering that Google has a net income of $32 million *a day*, $7 million is properly considered pocket change.[150] Thus, critics point out that the fines are not hefty enough and thus do not have a deterrent effect on these massive companies. Although, as David Vladeck, the former Director of the Bureau of Consumer Protection of the FTC and professor of law at Georgetown put it, "It is the public opprobrium, not the money, that counts in these cases."

Conclusion

As we look to the future, novel privacy issues are certain to arise. In the debate over who should address these privacy concerns, state attorneys general offices emerge as best positioned to tackle these concerns. State attorneys general should lead the strategy for enforcing these privacy rights, as they have since privacy rights emerged on the national scene. They are uniquely positioned to effectively lobby such legislation as they have successfully done in the past. Especially with the adoption of legislation modeled after the CCPA and CPRA, state

[148] Dishman at 845.
[149] Malathi Nayak, *9 States Criticize Google's Street View $13M Privacy Settlement*, Insurance Journal (January 28, 2020), https://www.insurancejournal.com/news/national/2020/01/28/556630.htm.
[150] Streitfeld, *supra* note 43.

attorneys general offices nationwide can pursue reasonable privacy measures for residents of their state. California is a model of the idea of states as laboratories of democracy through the promulgation of the CCPA and CPRA which have changed the landscape of privacy rights in the United States. As new data privacy issues arise, the state attorneys general offices can rely on existing consumer protection laws, legislation modeled after the CCPA, and lobby the legislature to adopt new legislation to address novel harms. Further, they can rely on multistate advocacy to obtain settlements which change the data privacy landscape through their terms. Although millions of Americans' data privacy harms are infringed, these individuals themselves cannot effectively seek redress. Only state attorneys general have the resources, the authority, and the capacity to protect Americans' privacy rights.