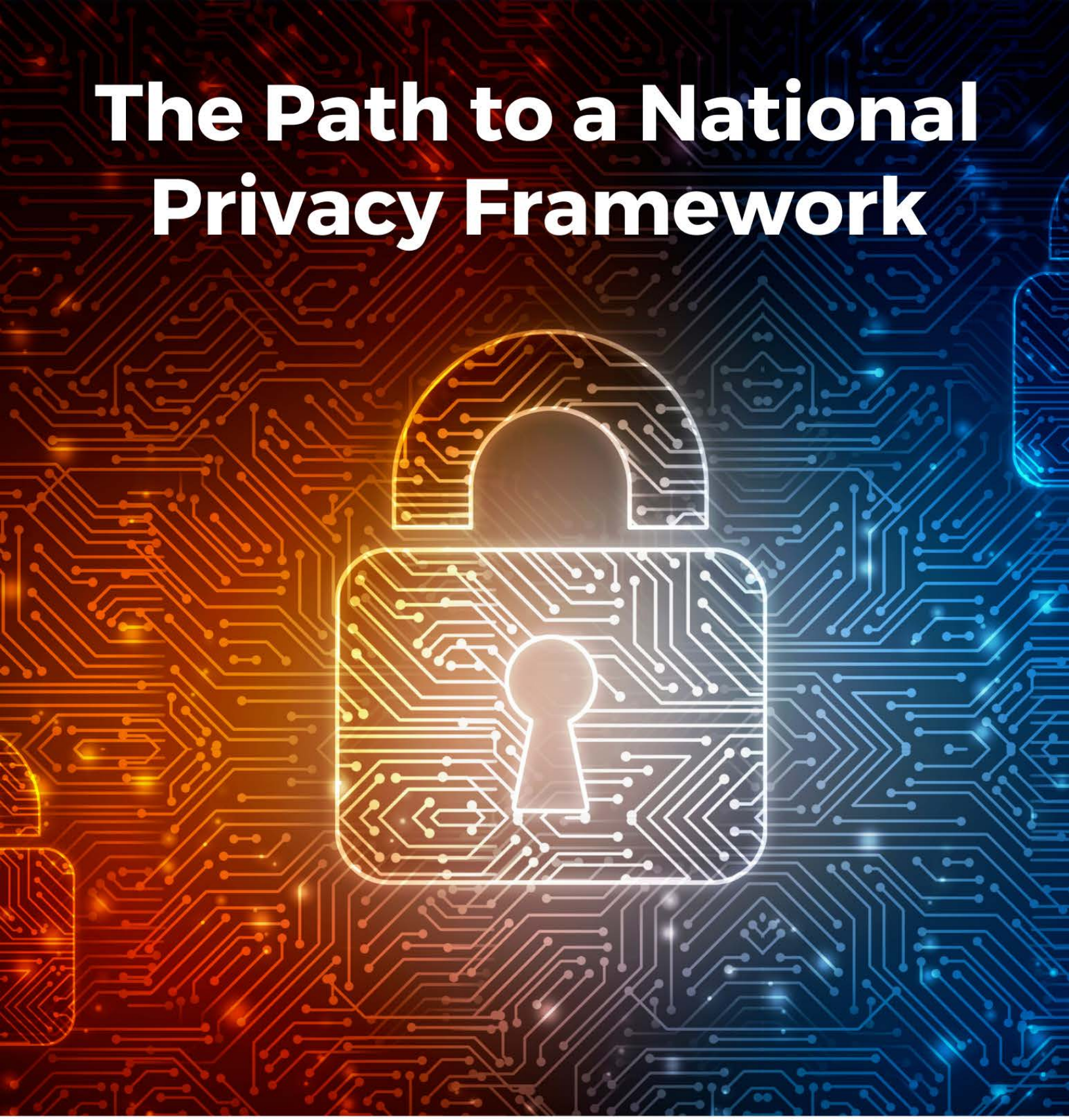
The Path to a National Privacy Framework



MARCH 2022

Deborah Collier
Ryan Lanier
Thomas Schatz

CITIZENS AGAINST GOVERNMENT WASTE

1100 Connecticut Ave, N.W. Suite 650
Washington, D.C. 20036
www.cagw.org

About CAGW

Citizens Against Government Waste (CAGW) is a private, nonprofit, nonpartisan organization dedicated to educating the American public about waste, mismanagement, and inefficiency in government.

CAGW was founded in 1984 by J. Peter Grace and nationally syndicated columnist Jack Anderson to build public support for implementation of the Grace Commission recommendations and other waste-cutting proposals. Since its inception, CAGW has been at the forefront of the fight for efficiency, economy, and accountability in government.

CAGW has more than 1 million members and supporters nationwide. Since 1984, CAGW and its members have helped save taxpayers more than $2.3 trillion. CAGW publishes special reports, including the *Congressional Pig Book* and *Prime Cuts*, as well as its official newsletter *Government WasteWatch* and blog *The WasteWatcher*, to expose government waste and educate the American people on what they can do to stop the abuse of their hard-earned money. Internet, print, radio, and television news outlets regularly feature CAGW's publications and experts.

Deborah Collier, Vice President of Policy and Government Affairs
Ryan Lanier, State Government Affairs Associate
Thomas Schatz, President

CITIZENS AGAINST GOVERNMENT WASTE

1100 Connecticut Avenue, N.W.
Suite 650
Washington, D.C. 20036
(202) 467-5300
www.cagw.org

The Path to a National Privacy Framework

Introduction

Beginning with the Communications Act of 1934,[1] which provided protection for telephone and cable customers' private information, several laws have been passed by Congress to protect data privacy and personal information. They include the Financial Modernization Act of 1999 (Gramm-Leach-Bliley Act) which regulates privacy for banking, credit reporting, and financial wire transactions;[2] the Children's Online Privacy Protection Act (COPPA), which protects children engaging in online activities;[3] the Driver's Privacy Protection Act of 1994, which prohibits the release of personal information by state agencies on drivers registered within their states;[4] the Electronic Communications Privacy Act of 1986 (ECPA) which regulates the access and use of electronic communications by law enforcement;[5] the Family Educational Rights and Privacy Act (FERPA), enacted in 1974, which protects the privacy of student information for secondary and college students and their families;[6] the Healthcare Insurance Portability and Accountability Act of 1996, which protects a patient's personal healthcare information;[7] and the Video Privacy Protection Act of 1988 (VPPA), which prohibits the disclosure of video rental records that contain personally identifiable information (PII).[8]

But as the amount of data held by private corporations like banking institutions, e-commerce sites, internet service providers (ISPs), online platforms, and retailers, among others, has increased exponentially, there is now a need to both update these laws, many of which are more than 30 years old, and develop a comprehensive federal data privacy framework.

The failure by Congress to accomplish this objective has led to many states enacting or considering their own data privacy laws and regulations. This conflicting, confusing, and complex hodgepodge approach is leaving consumers and businesses struggling to decipher what they need to do based on where they are located, and uncertainty about whether consumers have adequate protection under current law should their identities or other personal information be disclosed without their permission either through deliberate or accidental disclosures.

As technology becomes even more integrated into everyday life, it is more critical than ever that Congress devise a national framework for consumer data privacy that is flexible enough to meet the needs of consumers, provides certainty for businesses, and can be adapted for new innovations.

---

[1] Communications Act of 1934, Sections 222 and 227, https://transition.fcc.gov/Reports/1934new.pdf.
[2] Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act), Pub. L. No. 106-434, S. 900, https://www.congress.gov/bill/106th-congress/senate-bill/900.
[3] Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, Title XIII and Title XIV, Pub. L. No. 105-277, H.R. 4328, https://www.congress.gov/bill/105th-congress/house-bill/4328.
[4] Violent Crime Control and Law Enforcement Act of 1994, Title XXX, Pub. L. No. 103-322, H.R. 3355, https://www.congress.gov/bill/103rd-congress/house-bill/3355.
[5] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-647, H.R. 4952, https://www.congress.gov/bill/99th-congress/house-bill/4952.
[6] Elementary and Secondary Education Amendments, Pub. L. No. 93-380, Title V, H.R. 69, https://www.congress.gov/bill/93rd-congress/house-bill/69.
[7] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, H.R. 3103, https://www.congress.gov/bill/104th-congress/house-bill/3103.
[8] Video Privacy Protection Act of 1988, Pub. L. No. 100-618, S. 2361, https://www.congress.gov/bill/100th-congress/senate-bill/2361.

Privacy Laws and Regulations in Other Countries

The strictest privacy laws in the world, the General Data Protection Regulation (GDPR) were adopted by the European Parliament on April 14, 2016, and became directly applicable to all European Union (EU) member states on May 25, 2018. The GDPR imposes onerous and costly requirements for data protection by businesses or other entities that process the personal data of individuals in the member states of the EU, regardless of where the data processing takes place, including U.S. companies doing business in the EU.[9]

The GDPR has had a significant negative economic impact on countries and businesses in the EU. Jennifer Huddleston of the American Action Forum noted that, "venture capital investment in small and micro companies decreased by $3.4 million per week following GDPR's enactment" and such regulations have also had a negative impact on "other social priorities such as free speech."[10]

In her testimony before the Senate Judiciary Committee on March 12, 2019, American Enterprise Institute Visiting Scholar Roslyn Layton spotlighted 10 problems with the GDPR. She said that the regulations 1) strengthen the largest players; 2) weaken small- and medium-sized firms; 3) are cost prohibitive for many firms; 4) silence free speech and expression; 5) threaten innovation and research; 6) increase cybersecurity risk; 7) create risks for identity theft and online fraud; 8) reduce trust online; 9) use the pretense of customer control to increase the power of government; and, 10) fail to meaningfully incorporate the role of privacy enhancing innovation and consumer education in data protection.[11]

A CNBC report on the impact of the GDPR after one year of being in effect cited the struggles some EU countries faced as they tried staffing regulatory offices, and how "consumers become blind to an avalanche of privacy pop-up notices and companies struggle with new internal data bureaucracies."[12] In April 2020, *The New York Times* noted that "even the law's biggest supporters are frustrated with how it has worked."[13]

An additional burden on U.S. companies trying to comply with the GDPR, is the matter of data transfers from EU-member countries to non-EU member countries. This is particularly true for U.S.-based countries that have physical presence in EU countries and are capable of transferring data from a server located in the EU to a server based in the U.S., even if that data transfer is temporary or for performing backup storage for maintenance purposes. On July 16, 2020, the

---

[9] Roslyn Layton, "The GDPR: What It Really Does and How the U.S. Can Chart a Better Course," *Federalist Society Review*, Volume 19, October 29, 2018, https://fedsoc.org/commentary/publications/the-gdpr-what-it-really-does-and-how-the-u-s-can-chart-a-better-course.

[10] Jennifer Huddleston, "The Price of Privacy: The Impact of Strict Data Regulations on Innovation and More," American Action Forum, June 3, 2021, https://www.americanactionforum.org/insight/the-price-of-privacy-the-impact-of-strict-data-regulations-on-innovation-and-more/.

[11] Rosyln Layton, "Statement before the Senate Judiciary Committee on the General Data Protection Regulation and California Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation," U.S. Senate Judiciary Committee, March 12, 2019, https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony1.pdf.

[12] Kate Fazzini, "Europe's sweeping privacy rule was supposed to change the internet, but so far it's mostly created frustration for users, companies, and regulators," CNBC, May 5, 2019, https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html.

[13] Adam Satariano, "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates," *The New York Times*, April 27, 2020, https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html.

European Union Court of Justice (ECJ) issued a decision in *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems,* Case C-311/18 (*Schrems II).* In its ruling, the court determined that standard contractual clauses deemed whether the recipient country's law concerning government access to data meets the privacy protections under GDPR. The ECJ also invalidated the Privacy Shield Frameworks agreement, which had set up a mechanism to transfer personal data from the EU to the U.S.[14]

In September 2020, Department of Commerce Deputy Assistant Secretary for Services James M. Sullivan issued an explanatory letter on the impact and challenges of *Schrems II* on U.S. companies along with a white paper discussing how companies might be able to navigate the current data privacy standard until a new agreement can be forged.[15] On July 8, 2021, the Information Technology & Innovation Foundation (ITIF) released a report on how *Schrems II* has undermined sharing agreements between countries and imposed a certain level of distrust of service providers based in the U.S. The report encouraged the EU and U.S. to resolve these issues quickly and formulate an agreement that will be sustainable into the future.[16]

On March 25, 2022, President Biden and European Commission President Ursula von der Leyen announced that a provisional agreement had been reached that recognized the ECJ's decision and provided stronger legal protections for data transfers.[17] Whether this agreement will develop into a permanent resolution for data privacy concerns that will satisfy both businesses and privacy advocates remain to be seen.

Privacy Laws and Regulations in the States

Despite the clear problems with the GDPR, the state of California decided it would be a good model for its own data privacy laws. On June 28, 2018, the California Consumer Privacy Act (CCPA) was signed into law by Gov. Jerry Brown (D).[18] The bill, which was rushed through the legislature in a few days, imposes extremely burdensome requirements on how companies must store and provide access to consumers' personal information, as well as harsh restrictions on the types of product and service options and discounts companies may offer to their customers.

The CCPA also includes a private right of action, which gives individuals the ability to file suit against any company they believe violated their privacy rights. As a result, businesses could be held hostage by thousands of single lawsuits that threaten to bankrupt them. The private right of action and other harmful provisions of the CCPA underscore the risks of other states passing similar legislation.

---

[14] International Trade Administration, U.S. Department of Commerce, "Privacy Shield Overview," https://www.privacyshield.gov/Program-Overview.
[15] U.S. Department of Commerce, Letter from Deputy Assistant Secretary James Sullivan on the Schrems II Decision, September 2020, https://www.commerce.gov/about/letter-deputy-assistant-secretary-james-sullivan-schrems-ii-decision.
[16] Nigel Cory, "How 'Schrems II' Has Accelerated Europe's Slide Toward a De Facto Data Localization Regime," Information Technology & Innovation Foundation, July 8, 2021, https://itif.org/publications/2021/07/08/how-schrems-ii-has-accelerated-europes-slide-toward-de-facto-data.
[17] Francesco Guarascio and Foo Yun Chee, "EU-U.S. data transfer deal cheers business, but worries privacy activists," Reuters, March 25, 2022, https://www.reuters.com/legal/litigation/eu-us-reach-preliminary-deal-avoid-disruption-data-flows-2022-03-25/.
[18] Title 1.81.5, California Consumer Privacy Act of 2018, [1798.100 – 1798.199.100] (*Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3*), http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

The rush to pass CCPA forced the legislature to enact two bills to clarify and correct several problems. The first bill, AB 713, provided exceptions for data that had been "deidentified in accordance with specified federal law."[19] The second bill, AB 1281, extended exemptions to information collected by a business from job applicants, employees, owners, directors, officers, medical staff members, and contractors in addition to information related to a "written or verbal communication or transaction between a business and a consumer."[20]

On November 3, 2020, California voters approved Proposition 24, which adopted the California Privacy Rights Act (CPRA).[21] CPRA amends the CCPA to extend employee and business to business (B2B) exemptions for personal information; creates a higher threshold for the definition of a business effective January 1, 2023; creates a new definition for "sharing" personal information for "cross-context behavioral advertising;" includes the right to op-out; and requires the inclusion of a "Do Not Sell or Share My Personal Information" link. CPRA also imposes limits on the use of sensitive personal information like those imposed by the GDPR; creates new notice requirements at the point of data collection; imposes new requirements on service provider agreements; expands private rights of action; improves exemptions for clinical trials; and creates a new state agency dedicated to privacy enforcement, funded with $5 million for 2020-2021 and $10 million each following year.[22]

The state of Florida and its residents have made it quite clear that they do not want to be anything like California. It was therefore surprising that the normally pro-business and fiscally conservative Republican majority House of Representatives passed HB 9 by a vote of 102-8 on March 2, 2022.[23] The data privacy bill includes restrictive and burdensome provisions that are similar to the CCPA, including a private right of action.

A Florida TaxWatch analysis found that HB 9 provides 10 new privacy restrictions and would cut Florida's gross operating surplus by $17.2 billion annually.[24] The cost of compliance would have a disproportionate impact on small businesses that lack the resources to pay for the new restrictions. Entrepreneurs would be less inclined to choose Florida as the place to grow their new companies when faced with high start-up and compliance costs. Instead, they would choose states with more reasonable data privacy laws.

The complexity and cost of complying with HB 9 were compounded further by the inclusion of a private right of action. This right would result in frivolous lawsuits against every type of

[19] California Consumer Privacy Act of 2018, AB 713, 2019-2020 Legislative Session (2019), State Assembly, https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201920200AB713.
[20] Privacy: California Privacy Act of 2018, AB 1281, 2019-2020 Legislative Session (2019), State Assembly, https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=201920200AB1281.
[21] Secretary of State Alex Padillo, "California General Election Results," Tuesday, November 3, 2020, https://www.sos.ca.gov/elections/prior-elections/statewide-election-results/general-election-november-3-2020/statement-vote.
[22] Steven A. Hengeli, Jr., "California Privacy Rights Act: Latest Update, Impact and Next Steps," *The National Law Review*, July 2, 2020, https://www.natlawreview.com/article/california-privacy-rights-act-latest-update-impact-and-next-steps.
[23] Consumer Data Privacy, HB 9, 2021-2022 Legislative Session (2022), Florida House of Representatives, https://www.myfloridahouse.gov/Sections/Bills/billsdetail.aspx?BillId=76556; Council for Citizens Against Government Waste, "CCAGW Urges Florida House Judiciary Committee to Oppose HB 9," February 9, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-alaska-house-judiciary-committee-oppose-hb-159.
[24] Florida TaxWatch, "The Impacts of Consumer Data Privacy on Florida's Economy: A Detailed Look at HB 9 and SB 1864," February 22, 2022, https://floridataxwatch.org/Research/Full-Library/ArtMID/34407/ArticleID/19145/The-Impacts-of-Consumer-Data-Privacy-on-Florida's-Economy.

business in Florida, from large companies to the local pharmacy and grocery store, if someone thinks their privacy may have been violated. These types of provisions are a gold mine for trial lawyers, and a nightmare for businesses.

Even if a business is ultimately victorious, it would be difficult to recoup the time, money and reputation loss spent in needless litigation. The increased costs will be shifted to consumers, who end up paying higher prices for goods and services. Like the CCPA, the strict regulations and high compliance costs of HB 9 would make it more difficult for businesses to provide their products to consumers and protect the privacy of their customers, while also increasing barriers to entry. Fortunately for Florida businesses and taxpayers, HB 9 was not considered by the Senate before the legislative session ended on March 14, 2022, and it will not become law in the state.

On the opposite end of the spectrum of state laws stand Virginia's Consumer Data Protection Act (CDPA), which was signed into law by Gov. Ralph Northam (D) on March 31, 2020,[25] and the Colorado Privacy Act (CPA), signed into law by Gov. Jared Polis (D) on July 8, 2021.[26] These laws contain clear guidelines, limitations on the type and amount of data collected based on the context of the situation, consumer consent, opt-out clauses, and flexible levels of protection. Further, the CPDA and CPA do not contain a private right of action, or the stricter requirements featured in California's data privacy laws. In many ways, Virginia and Colorado stand out among the best examples of data privacy laws enacted at the state level. However, these laws remain state-based and therefore do not achieve the goal of protecting consumer data privacy with a single law that covers every state.

And despite their positive provisions, the CDPA and CPA have their differences. While some states may adopt some of these provisions, there is no guarantee that they will adopt the precise language. Other states may choose to follow the more burdensome model of California or the GDPR when crafting data privacy legislation. This wide variety of approaches makes it extremely difficult for consumers and businesses, particularly small businesses, to navigate the complex nuances of so many different laws.

In addition to California, Colorado, Florida, and Virginia, numerous other states have considered bills covering data brokers and consumer data privacy over the past several years. During the 2022 legislative sessions, they included Alaska's HB 159,[27] Connecticut's SB 6,[28] Hawaii's SB

[25] Consumer Data Protection Act, SB 1392, 2021 First Special Session (2021), Senate, https://lis.virginia.gov/cgi-bin/legp604.exe?211+sum+SB1392.
[26] Colorado Privacy Act, SB 190, 2021 Legislative Session (2021), Senate, https://leg.colorado.gov/bills/sb21-190.
[27] HB 159, 2022 Legislative Session, (2022) House, http://www.akleg.gov/basis/Bill/Detail/32?Root=HB159.
[28] An Act Concerning Personal Data Privacy and Online Monitoring, SB 6, 2022 Legislative Session (2022), Senate, https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&bill_num=SB00006&which_year=2022; Council for Citizens Against Government Waste, "CCAGW Urges Connecticut General Assembly Joint Law Committee to Oppose SB 6," March 2, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-connecticut-general-assembly-joint-general-law.

2051,[29] Indiana's SB 358,[30] Ohio's HB 376,[31] Oklahoma's HB 2969,[32] New Hampshire's HB 1413,[33] Wisconsin's AB 957,[34] Washington's SB 5813,[35] and Utah's SB 227,[36] and the Council for Citizens Against Government Waste wrote letters to the legislatures on each of these bills. There are unique provisions and applications that make each bill distinct from the others. For example, New Hampshire's HB 1413 singles out only one industry, broadband providers, whereas Hawaii's SB 2051 applies to data brokers more broadly. While those two bills focus on data brokering, others do not address data brokering at all. Other bills cover consumer and business privacy concerns, including the brokering of data. If these bills were all enacted into law, companies and consumers would find it extremely difficult and costly to comply.

The impact on smaller companies will be particularly damaging, as they may choose not to operate in states like California while still maintaining a presence in Colorado and Virginia, or states that do not have any data privacy laws. Consequently, consumers in many states will not have access to the same innovations as their friends and neighbors across state lines. Moreover, consumers will be confused over what is protected and what rights they have any time they engage in interstate travel or conduct online activities to purchase goods and services.

---

[29] HB 2051, 2022 Legislative Session (2022), House, https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=HB&billnumber=2051&year=2022; Council for Citizens Against Government Waste, "CCAGW Urges Hawaii House Higher Education and Technology Committee to Oppose HB 2051," February 1, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-hawaii-house-higher-education-and-technology-committee.

[30] SB 358, 2022 Legislative Session (2022), Senate, http://iga.in.gov/legislative/2022/bills/senate/358/; Council for Citizens Against Government Waste, "CCAGW Urges Indian House Commerce, Small Business, and Economic Development Committee to Oppose SB 358," February 15, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-indiana-house-commerce-small-business-and-economic.

[31] HB 376, 2022 Legislative Session (2022), House, https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA134-HB-376; Council for Citizens Against Government Waste, "CCAGW Urges Ohio House Government Oversight Committee to Oppose HB 376," February 8. 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-ohio-house-government-oversight-committee-oppose-hb-376.

[32] Oklahoma Computer Data Privacy Act, HB 2969, 2022 Legislative Session (2022), House, http://www.oklegislature.gov/BillInfo.aspx?Bill=hb2969&Session=2200; Council for Citizens Against Government Waste, "CCAGW urges Oklahoma House Technology Committee to Oppose HB 2969," February 15, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-oklahoma-house-technology-committee-oppose-hb-2969.

[33] HB 1413, 2022 Legislative Session (2022), House, https://gencourt.state.nh.us/bill_status/legacy/bs2016/bill_status.aspx?lsr=2754&sy=2022&sortoption=&txtsessionyear=2022&txtbillnumber=HB1413; Council for Citizens Against Government Waste, "CCAGW Urges New Hampshire House Commerce and Consumer Affairs Committee to Oppose HB 1413," February 7, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-new-hampshire-house-commerce-and-consumer-affairs.

[34] AB 957, 2022 Legislative Session (2022), State Assembly, https://docs.legis.wisconsin.gov/2021/proposals/reg/asm/bill/ab957; Council for Citizens Against Government Waste, "CCAGW Urges Wisconsin House Consumer Protection Committee to Oppose AB 957," February 15, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-wisconsin-house-consumer-protection-committee-oppose-ab.

[35] SB 5813, 2022 Legislative Session (2022), Senate, https://app.leg.wa.gov/billsummary?BillNumber=5813&Year=2021&Initiative=false; Council for Citizens Against Government Waste, "CCAGW urges Washington Senate Committee on Environment, Energy, and Technology to Oppose SB 5813," January 19, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-washington-senate-committee-environment-energy-and.

[36] Consumer Privacy Act, SB 227, 2022 Legislative Session, Senate, https://le.utah.gov/~2022/bills/static/SB0227.html; Council for Citizens Against Government Waste, "CCAGW Urges Utah Senate Revenue and Taxation Committee to Oppose SB 227," February 22, 2022, https://www.ccagw.org/legislative-affairs/state-action/ccagw-urges-utah-senate-revenue-and-taxation-committee-oppose-sb.

The Path to a National Privacy Framework

According to a January 24, 2022, ITIF report, a 50-state patchwork of laws would cost $1 trillion more over 10 years than if Congress enacted a national data privacy law.[37] The report found that under California's law alone, out of state compliance costs would total an estimated $12.5 billion while in-state compliance costs would total $46.4 billion. Businesses are going to be forced to raise prices to pay for these additional costs, and they will be passed on to consumers, or they will simply not do any business in California. Rather than allow this costly and confusing patchwork of laws to continue, Congress should use its power under the Commerce Clause of the Constitution to establish a unified framework for the entire nation.

Past Federal Legislation

In 2012, Citizens Against Government Waste (CAGW) reported on efforts to develop a set of national consumer privacy protection laws as reports about the tracking and monitoring of consumers' online use by companies and government entities increased.[38] Former President Barack Obama encouraged Congress to enact a modern set of privacy rules, offering a draft proposal for a Consumer Privacy Bill of Rights Act.[39] Yet 10 years later, Congress has still not modernized consumer privacy laws, or enacted a Consumer Privacy Bill of Rights.

Updating laws related to electronic communications is essential to keep up with modern technology. The Electronic Communications Privacy Law (ECPA), enacted in 1986, was one of the first laws to protect electronic communications. It has rapidly become outdated, as the manner in which documents and other digital "papers" are stored has evolved and online data and cloud storage solutions for electronic communications and documents have developed. ECPA fails to provide adequate protection for documents and communications stored remotely or by cloud service providers, including email, against unreasonable searches and seizures. Courts continue to struggle with how to apply the Fourth Amendment's protections, with the advent of newer communications platforms, even more so when dealing with myriad state and local laws being enacted to protect consumer privacy.

On July 27, 2017, Sens. Mike Lee (R-Utah), and Patrick Leahy (D-Vt.) introduced S. 1657, the ECPA Modernization Act of 2017. The Lee-Leahy bill would have amended ECPA by extending the same legal protections that data stored locally in one's home or office receives to information stored online. The process for obtaining a warrant would apply equally to all government agencies seeking access to content, which creates continuity and certainty for both businesses and individuals that may be subject to such a search for information. However, this legislation was not passed by either chamber of Congress.

During the 116th Congress, several bills to develop a national framework for consumer privacy were introduced in both the House and Senate, including H.R. 2013, the Information

---

[37] Sintia Radu, "50-State Patchwork of Privacy Laws Could Cost $1 Trillion More Than a Single Federal Law, New ITIF Report Finds," Information Technology and Innovation Foundation, January 24, 2022, https://itif.org/publications/2022/01/24/50-state-patchwork-privacy-laws-could-cost-1-trillion-more-single-federal.

[38] Deborah Collier, "Developing a Consumer Privacy Bill of Rights," *The WasteWatcher*, Citizens Against Government Waste, March 12, 2012, https://www.cagw.org/thewastewatcher/developing-consumer-privacy-bill-rights.

[39] National Archives, "Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015," The Obama White House Archives, February 23, 2012, https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

Transparency & Personal Data Control Act, introduced by Rep. Suzan K. DelBene (D-Wash.);[40] S. 2968, the Consumer Online Privacy Rights Act, introduced by Sen. Maria Cantwell (D-Wash.);[41] S. 3300, the Data Protection Act of 2020, introduced by Sen. Kirsten Gillibrand (D-N.Y.);[42] S. 3456, the Consumer Data Privacy and Security Act of 2020, introduced by Sen. Jerry Moran (R-Kans.);[43] and S. 4626, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (the SAFE DATA Act), introduced by Sens. Roger Wicker (R-Miss.), John Thune (R-S.D.), Marsha Blackburn (R-Tenn.), and Deb Fischer (R-Neb.).[44]

Again, these bills have not been enacted despite numerous hearings and town hall meetings to discuss the framework for a national privacy legislation.

Current Federal Legislation

During the 117th Congress, more than 30 bills have been introduced to address the nation's concerns about how personal identifying information is shared and used by those who collect data.[45] The bills demonstrate the bipartisan desire to protect consumers online, while at the same time offering a beginning framework for legislation that will work across all industries, and particularly for those that collect data online.

Unfortunately, there has been some confusion about whether a comprehensive data privacy bill should also include antitrust reform, revising or eliminating the consumer welfare standard, addressing online censorship and moderation, media rules, and breaking apart large technology companies. These are all different issues and have no place in a consumer data privacy law. Legislators working on consumer privacy should ignore the calls to include any of these matters, any one of which would likely lead to the defeat of such legislation. While has often proven difficult for Congress to pass legislation focused solely on one issue, members should focus only on one issue and work toward a national framework for consumer data privacy that will provide consumers and businesses a set of tools to protect data privacy.

Adding to the confusion, the Federal Trade Commission (FTC) has also been maneuvering toward taking up privacy rules as it attempts to streamlines its processes under Section 18 of the FTC Act.[46] However, as noted by Senate Commerce, Science, and Transportation Ranking Member Roger Wicker (R-Miss.), House Energy and Commerce Ranking Member Cathy McMorris Rogers (R-Wash.), and FTC Commissioner Noah Phillips, "This would be a step in

[40] Information Transparency & Personal Data Control Act, H.R. 2013, 116th Congress (2019), https://www.congress.gov/bill/116th-congress/house-bill/2013.
[41] Consumer Online Privacy Rights Act, S. 2968, 116th Congress (2019), https://www.congress.gov/bill/116th-congress/senate-bill/2968.
[42] Data Protection Act of 2020, S. 3300, 116th Congress (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3300.
[43] Consumer Data Privacy and Security Act of 2020, S. 3456, 116th Congress (2020), https://www.congress.gov/bill/116th-congress/senate-bill/3456.
[44] SAFE DATA Act, S. 4626, 116th Congress (2020), https://www.congress.gov/bill/116th-congress/senate-bill/4626.
[45] Müge Fazlioglue, "Privacy bills in the 117th Congress," International Association of Privacy Professionals (IAPP), August 24, 2021, https://iapp.org/news/a/privacy-bills-in-the-117th-congress/#.
[46] Alan Friel, Kristin Bryan and Kyle Fath, "FTC Issues Notice Contemplating Rulemaking for Security, Privacy and AI in 2022," Consumer Privacy World, Squire Patton Boggs, December 13, 2021, https://www.consumerprivacyworld.com/2021/12/ftc-issues-notice-contemplating-rulemaking-for-security-privacy-and-ai-in-2022/.

the wrong direction. America needs a national consumer privacy law, but such a law must be the product of Congress."[47]

In addition to the effort to add technology and telecommunications provisions to data privacy bills, several of the consumer privacy bills introduced during the 117th Congress have been related to COVID-19 and how information relating to vaccines and individual personal health information is managed. They cover contact tracing, vaccine passports, personally identifiable information (PII), and wearables.

These crisis-, industry-, and product-specific legislation will not solve the overreaching need for one standard consumer data privacy law that is vendor and industry neutral but provides the protection Americans want and need. Like the 116th Congress, there are several bills that have been introduced in the 117th Congress that seek to accomplish that objective.

On April 29, 2021, Sen. Jerry Moran (R-Kans.) introduced S. 1494, the Consumer Data Privacy and Security Act.[48] The legislation would "establish a clear federal standard for data privacy protection, giving businesses a uniform standard rather than a patchwork of confusing state laws; provide consumers with control over their own data to access , correct and erase their personal data; require businesses that collect and process a significant amount of personal data to take extra precautionary steps to protect and responsibly process that data; prohibit companies from collecting data without consumers' consent with limited and specific exceptions; require businesses to develop and implement robust data security programs to protect personal data from unauthorized access and disclosure; equip the FTC and state attorneys general with authority to uniformly enforce federal consumer privacy protections while providing the FTC the resources necessary to carry out those authorities.[49] This bill creates a baseline for hearings and additional bill discussions to help formulate a comprehensive national framework.

On November 1, 2021, Rep. Filemon Vela (D-Texas) introduced H.R. 5807, the DATA Privacy Act. H.R. 5807 establishes baseline data security requirements for businesses that collect, process, store, or disclose information on at least 50,000 individuals over a 12-month period. These businesses would be required to give consumers an accessible notice of the business's privacy practices relating to this information and appoint a privacy officer to oversee compliance of the privacy practices. The bill also requires the FTC to promulgate rules requiring businesses to limit why and how much consumer data is collected; provides consumers with the ability to opt-in or opt-out of data collection; gives consumers the ability to access, revise, transmit, and delete information collected about themselves, and establishes information security standards based on the sensitivity and identifiability of the collected data.[50]

---

[47] Sen. Roger Wicker, Rep. Cathy McMorris Rodgers, and Noah Phillips, "FTC Must Leave Privacy Legislating to Congress," *Washington Examiner*, September 29, 2021, https://www.washingtonexaminer.com/opinion/op-eds/ftc-must-leave-privacy-legislating-to-congress.

[48] Consumer Data Privacy and Security Act of 2021, S. 1494, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/senate-bill/1494.

[49] Sen. Jerry Moran, "Sen. Moran Introduces Bill Creating Clear Federal Standard for Consumer Data Privacy," News Releases, April 29, 2021, https://www.moran.senate.gov/public/index.cfm/2021/4/sen-moran-introduces-bill-creating-clear-federal-standard-for-consumer-data-privacy.

[50] DATA Privacy Act, H.R. 5807, 117th Congress (2021), https://www.congress.gov/bill/117th-congress/house-bill/5807.

The Path to a National Privacy Framework

On November 3, 2021, Reps. Cathy McMorris Rogers (R-Wash.) and Gus Bilirakis (R-Fla.) announced draft legislation, entitled the Control Our Data Act, which would promote innovation, increase transparency and accountability, create a clear set of rules for protecting consumers' data privacy.[51] The bill draft includes flexibility to account for large businesses and entities that have the means to invest in consumer data privacy, as well as small to mid-sized entities (SMEs) to protect them from undue regulatory burdens. Based on four principles for consumer data privacy that acknowledge that the internet does not stop at state lines, therefore there should be one standard set of rules for the entire country; people need to understand how their information is collected, used, and shared, and companies that misuse this information must be held accountable; federal legislation must ensure companies are implementing reasonable measures to protect individuals' PII; and, small businesses and innovation must be protected with a standard privacy law that is not overreaching, forcing businesses to hire attorneys instead of innovating.[52] As of publication date, the final text of this draft bill has yet to be introduced in the 117th Congress.

It can be expected that more legislation will be drafted and introduced during the second session of the 117th Congress. However, if legislation is going to pass, representatives and senators must come to an agreement quickly to move forward on building a consensus with a bipartisan agreement that will work nationwide.

CAGW's Recommendations for Consumer Data Privacy

On November 8, 2018, CAGW offered the following recommendations for consumer-based privacy to the National Telecommunications and Information Administration, which can also serve as a guide for any legislative initiative undertaken by Congress:

1. "National Privacy Framework: Because of the unique nature of the internet ecosystem and its presence beyond state borders, a clear and concise national data privacy framework is necessary to provide consistency and certainty for businesses and consumers alike.

2. "Consumer Choice and Control: Businesses should provide consumers with easy-to-understand privacy choices based on the sensitivity of their personal data and how it will be used or disclosed, consistent with the FTC's privacy enforcement guidance. Businesses should provide consumers with an opt-out choice to use their non-sensitive customer information for personalized third-party marketing. Businesses should be able to continue to rely on implied consent to use customer information for activities such as service fulfillment and support, fraud prevention, market research, product development, network management and security, compliance with the law, and first-party marketing.

[51] House Energy and Commerce Committee Republicans, "E&C Republicans Unveil Comprehensive Strategy to Establish a National Privacy Standard," November 3, 2021, https://republicans-energycommerce.house.gov/news/press-release/ec-republicans-unveil-comprehensive-strategy-to-establish-a-national-privacy-standard/.
[52] Ibid.

3. "Transparency: Consumers should be provided with clear, comprehensible, accurate, and continuously available privacy notices by businesses collecting, using, or sharing consumer data that describe in detail the information being collected, how that information will be used, and whether the information will be sold or shared with third parties. Should customer information be sold or shared with a third party, customers must be notified about the types of third parties to whom their information has been given and for what purpose.

4. "Data Minimization and Contextuality: Consumers should expect reasonable limits on the amount of personal data that organizations will collect, use, and disclose, consistent with the context in which that data is provided. Every effort should be made to de-identify and delete data as promptly as possible when it is no longer necessary.

5. "Flexibility: Different types of data require separate methods and standards of protection. For example, sensitive health care data and financial data require a higher level of security than a social media account or a computer's IP address. Therefore, policies must be consistent with the type of data being collected and how it is to be used.

6. "Data Security and Breach Notification: Consumers should expect that the personal data they share with other entities is maintained in a secure environment. Information technology systems are under constant attack; breaches have and will continue to occur. In the event of a data breach in which there is a reasonable likelihood of misuse and consumer harm, consumers should expect timely notification of the event, and an offer by the entity breached as to the remedies available to make the consumer as whole as possible, including credit protection services, fraud alerts, and credit monitoring through credit reporting agencies."[53]

These six recommendations provide the groundwork for a national privacy policy going forward, in a technology- and industry-neutral manner, and should be part of the overall privacy framework discussion. A national data privacy law must preempt these state-based laws while providing consumers the protections they need and enabling businesses to follow one set of standards without worrying about whether their customers have crossed a state boundary.

[53] Citizens Against Government Waste, "Comments to NTIA on Developing the Administration's Approach to Consumer Privacy," November 2, 2018, https://www.ccagw.org/legislative-affairs/agency-comments/comments-ntia-developing-administrations-approach-consumer.

Conclusion

It is long past time for Congress to enact a federal law to protect consumers' personal information. The patchwork of state laws that have been enacted and are being considered are making it costly and difficult for consumers and businesses to comply. Congress has the ability to solve this problem, but members need to act and move forward quickly on one of the bills that has been introduced or a combination thereof and put together a national framework for privacy protection that will simplify compliance, protect individual personal data, and encourage continued innovation.