The UNIVERSITY of VERMONT
Vermont Legislative Research Service
https://www.uvm.edu/cas/polisci/vermont-legislative-research-service-vlrs

Data Privacy Regulation

The US Federal Bureau of Investigation reported a record-setting $16.6 billion in US citizens' financial losses due to cybercrime in 2024, an increase of 33% from 2023. Of the nearly 860,000 complaints received, there was an average loss of $19,372 per complaint. Vermont State citizens filed 937 complaints and experienced around $11.3 million in losses. Countrywide, personal and corporate data breaches accounted for $1.8 billion of these losses.[1] Cybercriminals can use the information gathered from these breaches for further cybercrime by targeting identified individuals.[2]

All states in the European Union and 30 US states have introduced regulations to increase data privacy and security and establish consumer rights and protections in order to reduce the damage caused by these crimes. In a 2023 IBM report on data breaches within organizations around the globe, analysts identified noncompliance with regulations to be one of the top three factors amplifying the costs of a breach. They found a 23% difference, or $1.04 million, for the average cost of a breach between organizations with high levels of noncompliance compared to ones with low levels of noncompliance.[3]

This report summarizes several data privacy laws and examines the impact regulations have on businesses operations as well as the economic costs and social benefits.

Governmental Data Privacy Policies

Vermont

In 2018 the Vermont State Legislature passed Act No. 171, "An act relating to data brokers and consumer protection." The law provides Vermont consumers with information regarding the companies collecting their data and the companies' collection practices. The law also grants consumers the right to opt-out of this data collection and a right to a security freeze on their credit information without paying any fees. The bill defines data brokers as businesses that both collect and sell the information of consumers to which they do not have a direct relationship.

[1] Federal Bureau of Investigation, *Internet Crime Report,* 2024, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
[2] Australian Institute of Criminology, *Data Breaches and Cybercrime Victimisation,* November 2022, https://www.aic.gov.au/sites/default/files/2022-11/sb40_data_breaches_and_cybercrime_victimisation.pdf.
[3] IBM Security, *The Cost of a Data Breach Report 2023,* 2023, https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf.

This excludes businesses like banks and retail stores that only collect personal data from customers that use their services or buy their products.[4]

The law requires data brokers to register every year and adopt measures to increase data security. These measures include:

- Having a designated position dedicated to data security;
- Conducting ongoing training;
- Establishing procedures to identify potential risk;
- Procedures to evaluate how to improve security; and,
- Security policies for employees on safe data handling.

Consumers must file complaints on violations of these provisions with the Vermont Attorney General who has sole authority to bring civil action and collect penalties. Data brokers that fail to register will accrue a civil penalty of $50 per day, not to exceed $10,000 per year.[5]

Vermont H.208: The Vermont State Legislature is considering a bill to expand data privacy security, H.208, "An act relating to consumer data privacy and online surveillance." Modeled after the Connecticut Data Privacy Act (CTDPA), H.208 grants consumers the following rights regarding their personal data: the right to confirm, the right to know, the right to obtain, the right to correct, and the right to opt-out of any future data collection.[6] H.208 contains provisions that increase protection of personal health data, protection of minors, and expand regulation of data controllers and processors.

These provisions apply to persons that conduct business in Vermont or target products or services to Vermont consumers and who process or control the data of 25,000 or more consumers, or 12,500 or more consumers if sales of personal data account for 25% or more of their gross revenue.[7] Exemptions include controllers and processors that: collect health data but fall under the guidelines of HIPAA, use de-identified data which cannot be traced back to an individual, use personal data in order to evaluate credit worthiness, who's data use is already subject to other federal privacy regulation, non-commercial activity of public media such as publishers, newspapers, periodicals with regular circulation, and licensed radio and television.[8]

Consumers cannot take private civil action against a controller registered in Vermont that made less than $25 million in revenue the previous year. The Attorney General is required to provide the Vermont legislature with an annual report disclosing complaints, violations and civil actions taken, and data brokers and large data holders most frequently sued under the provisions of H.208. The Vermont Attorney General is responsible for issuing a fine of $10,000 per violation

[4] Vermont General Assembly, *An Act Relating to Data Brokers and Consumer Protection*, H.764, Enacted May 22, 2018, https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.
[5] Vermont General Assembly, *An Act Relating to Data Brokers and Consumer Protection*.
[6] For the purposes of this report the list of rights has been shortened, for the full list see The Vermont General Assembly, *An Act Relating to Consumer Data Privacy and Online Surveillance,* H.208, bill as introduced February 12, 2025, https://legislature.vermont.gov/Documents/2026/Docs/BILLS/H-0208/H-0208%20As%20Introduced.pdf § 2418.
[7] The Vermont General Assembly, *An Act Relating to Consumer Data Privacy and Online Surveillance.*
[8] The Vermont General Assembly, *An Act Relating to Consumer Data Privacy and Online Surveillance.*

if the violation cannot be fixed within the mandated 60-day cure period.[9] The bill grants consumers a civil right of action against data brokers and data handlers that processed the personal data of over 100,000 consumers in the previous year for violations of H.208 provisions which must be approved by the Attorney General.[10]

California

Legislators signed the California Consumer Privacy Act (CCPA) into law in June 2018 and made effective starting on January 1, 2020.[11] The first version of the bill included a set of new privacy rights for consumers, among them: the right to know, the right to delete, the right to opt-out, and the right to non-discrimination for exercising their CCPA rights.[12] It also included a 30 day 'cure period' for businesses to correct violations.[13] Following this initial bill, voters passed ballot initiative Proposition 24 in November 2020, which further strengthened the CCPA. The proposition added the right for consumers to correct inaccurate personal information and the right to limit the use and disclosure of sensitive personal information.[14] The bill was also renamed to the CPRA (California Privacy Rights Act).[15]

The CPRA applies to companies using three criteria:

1. Companies who have a gross revenue of at least $25 million annually;
2. Companies that buy, sell, or share the data of more than 100,000 consumers; and
3. Companies with 50 percent or more of their annual revenue from buying and selling consumer data.[16]

The penalties for violations are no more than $2,663 per accidental violation and $7,998 per intentional violation. Any violation involving a minor is automatically classed in the same bracket as an intentional violation.[17] Following the passing of the CPRA, the mandatory cure period was removed from the provision.[18]

---

[9] The Vermont General Assembly, *An Act Relating to Consumer Data Privacy and Online Surveillance*; See also 9 Vt. Stat. Ann. § 2461 for enforcement penalty.
[10] The Vermont General Assembly, *An Act Relating to Consumer Data Privacy and Online Surveillance.*
[11] California Privacy Protection Agency. *California Consumer Privacy Act of 2018* (Cal. Civil Code § 1798.100 et seq.). Effective January 1, 2025, https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf.
[12] California Department of Justice, Office of the Attorney General. "California Consumer Privacy Act (CCPA): Frequently Asked Questions (FAQs)." Last modified March 13, 2024. Accessed November 11, 2025. https://cdn.lawreportgroup.com/acuris/files/Cybersecurity-New/Gordon%20QA%20California%20Consumer%20Privacy%20Act%20(CCPA).pdf.
[13] California Department of Justice, "California Consumer Privacy Act (CCPA): Frequently Asked Questions (FAQs)."
[14] California Department of Justice, "California Consumer Privacy Act (CCPA): Frequently Asked Questions (FAQs)."
[15] California, Secretary of State, "Proposition 24: California Privacy Rights Act of 2020," in *Official Voter Information Guide, California General Election, November 3, 2020* (Sacramento: Secretary of State, 2020), 42–49, https://vig.cdn.sos.ca.gov/2020/general/pdf/complete-vig.pdf.
[16] California, Secretary of State, "Proposition 24: California Privacy Rights Act of 2020."
[17] California, Secretary of State, "Proposition 24: California Privacy Rights Act of 2020."
[18] California, Secretary of State, "Proposition 24: California Privacy Rights Act of 2020."

Though the attorney general is responsible for much of the enforcement of the CPRA, the measure also created the California Privacy Protection Agency.[19] The agency is responsible for enforcement usually through administrative proceedings, while the attorney general is responsible for civil suits. The attorney general still retains the last say on whether a company would be prosecuted for a violation. The largest suit to date was a $1.55 million settlement with Healthline.com for failing to allow consumers to opt out.[20]

New Hampshire

The New Hampshire Data Privacy Act (NHDPA) was signed into law in June of 2024 and made effective January 2025.[21] Like the CPPA, the NHDPA includes the right to know, the right to delete, the right to correct, and the right to opt-out.[22] The bill applies to companies who either process the data of 35,000 New Hampshire residents, or process the data of 10,000 New Hampshire residents and derive more than 25% of their annual revenue from the sale of personal data.[23] One of the bill's sponsors, State Senator Donna Stoucey, stated that the lower cutoff for the data comptrollers was to reflect the fact that New Hampshire is a smaller state.[24]

The penalties for violation are either civil or criminal penalties. A fine for a civil violation is $10,000 per violation, while a criminal penalty is $100,000. A criminal penalty is deemed to be a purposeful violation of the NHDPA, and this is left at the discretion of the attorney general.[25] In 2025, the NHDPA gives companies a mandatory cure period of 60 days to rectify the violation before the attorney general can press charges. Starting January 1st, that 'cure period' is left to the discretion of the attorney general's office.[26] The attorney general's office is responsible for the enforcement of NHDPA. In August of 2024, the attorney general announced the creation of a Data Privacy Unit, tasked with enforcing compliance with NHDPA.[27] The bill does not grant citizens a private right of action; all enforcement is done through the attorney general's office.

[19] California Privacy Protection Agency. "Laws & Regulations." Accessed November 12, 2025, https://cppa.ca.gov/regulations/.
[20] California Department of Justice. "Attorney General Bonta Announces Largest CCPA Settlement to Date, Secures $1.55 Million from Healthline.com." Press release, July 1, 2025, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155.
[21] New Hampshire General Court, *Senate Bill 255, 2024 Regular Session*, PDF, New Hampshire General Court, https://gc.nh.gov/bill_status/legacy/bs2016/billText.aspx?sy=2024&id=865&txtFormat=pdf&v=current.
[22] New Hampshire General Court, *Senate Bill 255, 2024 Regular Session*.
[23] New Hampshire Secretary of State, *RSA 507-H as Amended by Ch 229*, PDF, New Hampshire Secretary of State, https://www.sos.nh.gov/sites/g/files/ehbemt561/files/inline-documents/sonh/rsa-507-h-as-amended-by-ch-229.pdf.
[24] Duball, Joe. "State Lawmaker's Take on New Hampshire Comprehensive Privacy Bill's Impacts." *IAPP*, January 22, 2024 https://iapp.org/news/a/state-lawmakers-take-on-new-hampshire-comprehensive-privacy-bills-impacts/.
[25] New Hampshire Department of Justice. "Attorney General Formella Announces Creation of New Data Privacy Unit." Press release, August 15, 2024, https://www.doj.nh.gov/news-and-media/attorney-general-formella-announces-creation-new-data-privacy-unit.
[26] Duball, Joe. "State Lawmaker's Take on New Hampshire Comprehensive Privacy Bill's Impacts." *IAPP*, January 22, 2024.
[27] New Hampshire Department of Justice, Office of the Attorney General, "Attorney General Formella Announces Creation of New Data Privacy Unit," press release, August 15, 2024.

Connecticut

The Connecticut Data Privacy Act (CTDPA) was enacted in May 2022 and made effective in July 2023.[28] The bill grants consumers the right to access, the right to correct, the right to delete, right to data portability, right to opt-out, and the right to appeal.[29] The businesses subject to regulation under the CTDPA either process the data of 100,000 or more Connecticut residents, or control or process the data of at least 25,000 residents and derive more than 25% of their gross revenue from the sale of personal data.[30]

The attorney general, who is solely responsible for enforcing CTDPA, is required to give companies a 60-day cure period. That provision of the bill expired January 1, 2025, after which any cure period is at the discretion of the attorney general.[31] The penalties for non-compliance are $5,000 per willful violation, as well as restitution, disgorgement, and injunctive relief at the discretion of the attorney general.[32] There is no private right of action under the CTDPA. In July 2025, TicketNetwork was forced to pay $85,000 in a civil suit for violating the CTDPA, the only fine issued under the CTDPA so far.[33]

European Union

The European Union passed The General Data Protection Regulation (GDPR) in2018.[34] The GDPR's protections apply to all personal data. The bill refers to these protections as 'digital rights', and among them are:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restriction;
- the right to data portability;
- the right to object; and,
- the right to non-automated decision making.[35]

All subjects of the European Union possess these digital rights.

---

[28] Connecticut General Assembly. *An Act Concerning Personal Data Privacy and Online Monitoring* (Public Act No. 22-15). 2022. https://www.cga.ct.gov/2022/act/pa/pdf/2022PA-00015-R00SB-00006-PA.pdf.
[29] Connecticut General Assembly. *An Act Concerning Personal Data Privacy and Online Monitoring*.
[30] Connecticut Office of the Attorney General. "The Connecticut Data Privacy Act." Accessed November 11, 2025. https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act.
[31] Connecticut General Assembly. *An Act Concerning Personal Data Privacy and Online Monitoring*.
[32] Connecticut Office of the Attorney General, "The Connecticut Data Privacy Act."
[33] Office of the Attorney General, State of Connecticut, "Attorney General Tong Announces $85,000 Settlement with TicketNetwork for Violations of the Connecticut Data Privacy Act," Press release, July 8, 2025, https://portal.ct.gov/ag/press-releases/2025-press-releases/attorney-general-tong-announces-settlement-with-ticketnetwork.
[34] *General Data Protection Regulation (GDPR) – Legal Text*, EU, accessed November 21, 2025, https://gdpr-info.eu/.
[35] Dylan Walsh, "GDPR Reduced Firms' Data and Computation Use," *MIT Sloan School of Management: Ideas Made to Matter* ", September 10, 2024, https://mitsloan.mit.edu/ideas-made-to-matter/gdpr-reduced-firms-data-and-computation-use.

The GDPR divides penalties for violations into two tiers based on which articles of the GDPR are breached. Higher tier penalties, which include violations of the subject's digital rights, incur a penalty of €20 million or 4% of annual revenue, whichever figure is higher. Lower tier penalties, including failure to report, incur a penalty of €10 million, or 2% of annual revenue, whichever figure is higher. As of 2024, there have been over $5 billion dollars in penalties, the largest of which being a $1.3 billion fine against Meta in 2023.[36]

Impacts of Data Regulation on Businesses, Markets

Required Operational Changes

According to research by Sourav et al., the implementation of data regulation has caused companies to handle data differently, shifting focus to transparency, accountability, and user consent.[37] In complying with data regulations, businesses face several challenges: following long and detailed laws, keeping operations efficient, and competing effectively. To strengthen their compliance, organizations must set up advanced safety in IT, work with lawyers, hire privacy staff, and train workers. If companies do not comply, they are subject to fines, and may lose their credibility, making them add data production to their risk of planning. Poor compliance with data storage can cause lawsuits, work disruptions, and a reduction of customers. These expenses are often higher than what it would cost to comply with the regulations.[38]

Companies that use detailed data to target customers, analyze how they act, and create AI models must now adapt their methods to be in accordance with rules around consent, reducing how much data is kept, and restricting uses for the data.[39] There is a clear link between the implementation of data privacy laws and changes in business operations worldwide. By late 2020, countries that adopted GDPR inspired polices early had invested more in compliance, improved their data management systems, and experienced fewer reports of data breaches.[40]

Competitive Advantages of Compliance

Complying with policy standards can help businesses win over competition. Businesses that focus on privacy engender higher trust among customers, develop improved governance of their data, and reduce the chance of data breaches; all of which produce better long-term financial

[36] Dylan Walsh, "GDPR Reduced Firms' Data and Computation Use," *MIT Sloan School of Management: Ideas Made to Matter,*" September 10, 2024.
[37] Sultanul Arefin Sourav, Imran Khan, and Tanvir Rahman Akash, "Data Privacy Regulations and Their Impact on Business Operations: A Global Perspective," *Journal of Business and Management Studies*, Vol. 2, no. 1(2020).
[38] Sourav et al., "Data Privacy Regulations and Their Impact on Business Operations."
[39] Mantelero, Alessandro, "Towards a New Dimension of Privacy and Data Protection in the Big Data Era." In *Group Privacy to Collective Privacy*, (Springer, 2016), https://doi.org/10.1007/978-3-319-46608-8_8.
[40] Sourav et al., "Data Privacy Regulations and Their Impact on Business Operations."

outcomes.[41] Companies that actively build and prioritize privacy over their organization stand a better chance of surviving and improving amid new global regulations.[42]

Market Concentration Effects

In the absence of standardized language, consumers often struggle to understand privacy notices.[43] This could give large firms an advantage over small firms, as their resources allow them to create clearer and more trustworthy privacy policies.[44] Larger companies create closed online platforms known as 'walled gardens', where content and user experience are tightly managed.[45] However, if regulations enforce standardized privacy notices, smaller firms could compete more effectively by reducing confusion and leveling the trust gap.[46]

Costs of Compliance

In the Standardized Regulatory Impact Assessment (SRIA) of the CCPA prepared for the California Attorney General's Office, analysts identified cost factors for businesses to comply with data privacy regulations. These included legal costs to interpret the laws to inform plans, operational costs to establish proper compliant practices including training and record keeping, technical costs to purchase or develop the technologies required to respond to consumers and meet security standards, and business costs associated with contracting and changing business models to meet data handling requirements.[47] A follow-up SRIA for California's 2024 privacy law changes identified risk assessments and security audits as an additional cost.[48]

Based on surveys and state data analysis, analysts for the CCPA assessment assumed an upper bound of 50-75% of businesses would fall within the parameters requiring regulation. Citing a TrustArc survey, analysts estimated initial costs incurred for small businesses of less than 20 employees would be $50,000, medium businesses of 20-100 employees would be $100,000, medium to large businesses of 100-500 employees would be $450,000, and large businesses of more than 500 employees would be $2,000,000.

---

[41] Von Grafenstein, Maximilian, "Co-regulation and competitive advantage in the GDPR: Data protection certification mechanisms, codes of conduct and data protection-by-design," In *Research Handbook on Privacy and Data Protection Law,* (Edward Elgar, 2022), https://doi.org/10.4337/9781786438515.
[42] Sourav et al., "Data Privacy Regulations and Their Impact on Business Operations."
[43] Avi Goldfarb and Catherine Tucker, "Privacy and Innovation," *Innovation Policy and the Economy,* Vol. 12 no. 1 (University of Chicago Press, 2012), https://www.researchgate.net/publication/350820467_Towards_creating_an_effective_customer_brand_engagement_through_social_media_marketing_A_model_proposal_2021 .
[44] Goldfarb and Tucker, "Privacy and Innovation."
[45] Goldfarb and Tucker, "Privacy and Innovation."
[46] Goldfarb and Tucker, "Privacy and Innovation."
[47] State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Protection Act of 2018 Regulations,* August 2019, https://dof.ca.gov/media/docs/forecasting/economics/major-regulations/major-regulations-table/CCPA_Regulations-SRIA-DOF.pdf.
[48] California Privacy Protection Agency, *Standardized Regulatory Impact Assessment: California Privacy Protection Agency,* August 2024, https://dof.ca.gov/media/docs/forecasting/economics/major-regulations/major-regulations-table/CPPA-SRIA-DOF.pdf.

The California Attorney General's Office estimated that 75% of businesses meeting the threshold for regulation, with analysts estimated that the total initial compliance cost for the over 570,000 effected companies would be $55 billion or roughly 1.8% of California's 2018 GSP.[49] Analysts note that this was calculated for the upper limit, and the costs would be higher for the first years of compliance. They estimated subsequent years to be 15-30% or year one compliance costs.[50] They also note many large companies have already adjusted to comply with the GDPR, likely reducing this amount. Based on decreasing yearly costs weighed against cost savings from reduction of cybercrime, not including unquantifiable benefits to consumers, analysts estimated that total compliance costs would be less than 0.1% of state GSP by 2030.[51]

A 2021 meta-analysis of compliance cost surveys found a wide range of yearly privacy costs depending on the study, the industry, and size of the business.[52] In one survey, the researchers found a median cost of around $200,000 in privacy costs for companies with under 5,000 employees increasing up to almost $1,000,000 for companies with over 75,000 employees. Another study cited found a higher average for GDPR compliance in 2019 at $13.6 million. The companies surveyed in these reports were mostly large multinational corporations.[53]

In a 2024 study on the effect of the GDPR examining data from 275,000 companies across three industries, researchers found that companies targeting EU markets saw a 2.1% decrease in profits correlated with GDPR compliance.[54] In a comparative study of US and EU data storage and processing, researchers documented that within two years after the implementation of the GDPR European companies decreased their data sensitivity by storing 26% less data and doing 15% less computation. As a result, the researchers measured a 20% increase in the variable cost (cost changes in relation to the amount of production/volume of services) of data due to the GDPR, however this only translated into a 3.5% increase in the variable cost of information and 0.1-0.5% total increase in production costs.[55]

Regulation Impact on Small and New Businesses

Even though total compliance costs are less for smaller businesses, their costs to revenue ratio along with their average cost per employee tend to be higher, and they often have fewer resources to interpret new regulations.[56] Fixed costs (costs that don't change with production

[49] State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Protection Act of 2018 Regulations.*
[50] California Privacy Protection Agency, *Standardized Regulatory Impact Assessment: California Privacy Protection Agency.*
[51] State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Protection Act of 2018 Regulations.*
[52] Anupam Chander, Meaza Abraham, Sandeep Chandy, Yuan Fang, Dayoung Park, and Isabel Yu, *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation*, World Bank Policy Research Working Paper 9594 (March 2021), https://scholarship.law.georgetown.edu/facpub/2374/.
[53] Chander et al., *Achieving Privacy: Costs of Compliance and Enforcement of Data Protection Regulation.*
[54] Carl Benedikt Frey and Giorgio Presidente, "Privacy regulation and firm performance: Estimating the GDPR effect globally," *Economic Inquiry,* Vol. 62 No. 3 (July 2024).
[55] Mert Demirer, Diego J. Jiménez Hernández, Dean Li, and Sida Peng, *Data Privacy Laws and Firm Production: Evidence from the GDPR,* National Bureau of Economic Research Working Paper 32146 (December 2024), https://www.nber.org/system/files/working_papers/w32146/w32146.pdf.
[56] Frey and Presidente, "Privacy regulation and firm performance."

levels) account for a greater percentage of total costs for small businesses, creating a disproportionate spending on compliance compared to larger businesses. Large businesses such as Google are able to absorb compliance costs by passing them down to their large consumer base through small price increases.[57]

In a study modeling privacy regulation's effect on market structure, researchers showed that specialized firms in markets that offer less price flexibility, such as internet advertising, are less able to absorb compliance costs through increasing prices. They note that an average price cap serves as a deterrent for market entry and having an opt-out mechanism in marketing further softens price competition. This results in regulation giving large corporations that offer a wider range of products and services greater comparative advantage in these markets.[58] Researchers in a 2021 study examining the market impacts of the GDPR quantify this shift showing websites have been choosing larger web service providers over smaller ones with a 15% decrease in third-party requests and a 17% increase in concentration in the market. They trace this increased concentration to dominant vendors' increase in market share.[59]

Effects of Privacy Regulation on Advertising

Personalization marketing using consumer data can facilitate the competitiveness of smaller businesses by targeting specific customer segments.[60] Privacy restrictions on search browsers such as Safari and Chrome remove this strategy, disproportionally harming smaller sellers, limiting their competitiveness.[61]

The ad industry relies on cross site/app identifiers, which include third-party cookie identifiers and mobile ad identifiers.[62] Cross-site/app identifiers create value for advertisers by improving targeting, measurement, and optimization.[63] This data, believed to be the "heart of effectiveness of digital advertising," has become difficult to track with the implementation of data privacy regulations.[64] The lack of cross-site data limits the information available to a third-party

---

[57] Christopher Bret Alexander, "The General Data Protection Regulation and California Consumer Privacy Act: The Economic Impact and Future of Data Privacy Regulations," *Loyola Consumer Law Review,* Vol. 32 no. 2 (2020).
[58] David Campbell, Avi Goldfarb, and Cathrine Tucker, "Price Regulation and Market Structure," *Journal of Economics & Management Strategy*, Vol. 24 no. 1 (Spring 2015).
[59] Christian Peukert, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer, "Regulatory Spillovers and Data Governance: Evidence from the GDPR," *Marketing Science,* Vol. 41 no.4 (February 2022).
[60]Ait Lamkadem et al., "Towards creating an effective customer brand engagement through social media marketing: A model proposal," *International Journal of Business and Management Invention,* vol. 10, (2021), https://www.researchgate.net/publication/350820467_Towards_creating_an_effective_customer_brand_engagement_through_social_media_marketing_A_model_proposal_2021
[61] Sultanul Arefin Sourav et al., "Data Privacy Regulations and Their Impact on Business Operations: A Global Perspective."
[62]Jean-Pierre Dubé et al. "Frontiers: The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing," Vol. 44 no. 5 (*Marketing Science,* 2025), https://doi.org/10.1287/mksc.2024.0901
[63] Jean-Pierre Dubé et al., "Frontiers: The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing."
[64] Jean-Pierre Dubé et al., "Frontiers: The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing."

advertiser.[65] This has the potential to disproportionately disadvantage smaller businesses, as nine out of ten small businesses predominantly use digital advertising.[66]

Wernerfelt et al. report on a large-scale randomized experiment using 70,000 advertising campaigns on Meta platforms that measure the incremental profits associated with the loss of offsite data.[67] Results indicated that over 90% of advertisers would experience an increase in the cost per incremental customer acquired through advertising if the campaign was limited to onsite data instead of offsite data. The smallest advertisers are harmed disproportionally more by the loss of access to offsite data.[68] The median small advertiser loses 25 incremental customers per $1,000 spent on advertising, while the median large advertiser only loses 5 customers.[69]

Privacy restrictions that limit or ban the use of data for advertising can increase the concentration in the advertising market. After the implementation of the GDPR, concentration in EU digital advertising markets increased, as did the market share for Google and Facebook.[70] This is because Apple's app tracking transparency (ATT) used different opt-in prompts for Apple versus third-party apps, potentially giving Apple higher opt-in rates and more access to targetable user data.[71]

Benefits of Privacy Regulations

In the Standardized Regulatory Impact Assessment (SRIA) of the California Consumer Privacy Act (CCPA) analysts cite studies showing a 90% consumer preference for control of their data and a 68% dislike of being tracked for targeted advertising. They add that benefits such as the value of security and trust and of having established rights are difficult to measure.[72] Studies have attempted to quantify the impact of increased data privacy regulation on consumer trust, but results have been mixed with some researchers finding a correlation while others finding none.[73]

---

[65] Jean-Pierre Dubé et al., "Frontiers: The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing."
[66] Jean-Pierre Dubé et al., "The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing: A Marketing Science Institute Report."
[67] Nils Wernerfelt, Anna Tuchman, Bradley T. Shapiro, and Robert Moakler, "Estimating the Value of Offsite Tracking Data to Advertisers: Evidence from Meta," *Marketing Science,* Vol. 44 no. 2 (2024).
[68] Jean-Pierre Dubé et al., "The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing: A Marketing Science Institute Report."
[69] Jean-Pierre Dubé et al., "The Intended and Unintended Consequences of Privacy Regulation for Consumer Marketing: A Marketing Science Institute Report."
[70] Christian Peukert, Stefan Bechtold, Michail Batikas, and Tobias Kretschmer, "Regulatory Spillovers and Data Governance: Evidence From the GDPR." *Marketing Science* vol 41 no.4 (2022).
[71] Sagar Baviskar, Iffat Chowdhury, Daniel Deisenroth, Beibei Li, and D. Daniel Sokol, "ATT Vs. Personalized Ads: User's Data Sharing Choices Under Apple's Divergent Consent Strategies." *USC* Center for Law and Social Science Research Paper Series No. 24-26 (January 2024): https://doi.org/10.2139/ssrn.4887872.
[72] State of California Department of Justice Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Protection Act of 2018 Regulations.*
[73] Study finding no correlation: Paul Bauer, Frederic Gerdon, Florian Keusch, Frauke Kreuter, and David Vannette, "Did the GDPR Increase Trust in Data Collectors? Evidence from Observational and Experimental Data," *Information, Communication & Society,* Vol. 25 no. 14 (May 2021); Study finding a correlation: Jingjing Zhang, Farkhondeh Hassandoust, and Jocelyne Williams, "Online Customer Trust in the Context of the General Data Protection Regulation," *Pacific Asian Journal of the Association for Information Systems,* Vol. 12 no. 1 (March 2020).

SRIA analysts do quantify financial benefits using savings from avoiding cybercrime. They estimated at 12.6% reduction in data related cybercrimes amounting to an aggregate of $66.3 billion in benefits for California by 2036.[74] State revenues from fines can be measured as economic benefits. Results from a 2025 fines and data breach survey showed the total GDPR revenue from fines collected since it was implemented in 2018 is $6.17 billion.[75] The regulation compliance service industry has grown with the implementation of the GDPR reaching a market cap of $4.44 billion in 2025, which is an increase of 25% from the previous year. These firms offering services for audits, assessments, and legal compliance have created new jobs and have been reducing the cost of compliance, particularly for smaller businesses.[76]

Summary

The financial losses suffered by US citizens and organizations due to cybercrime, highlighted by the FBI's record $16.6 billion loss in 2024, have rendered enhanced data privacy regulation an economic and social priority. While compliance demands significant initial and ongoing investment, estimated to be in the billions for major jurisdictions like California, these costs have been effective in securing data and are mitigated by savings from reduced cybercrime and the creation of a growing regulatory compliance service industry. However, data privacy regulation may negatively impact competition and increase market concentration. While compliance builds consumer trust, restrictions on offsite data tracking for advertisers tend to disproportionately harm smaller businesses and advertisers. Alongside this, larger corporations are often able to shoulder the initial financial burden for compliance. Some data regulation policies attempt to balance these competing incentives by maximizing data security while establishing well-defined cutoffs that ensure a competitive business environment.

This report was completed on December 9, 2025, by Skye Whalen, Kevin Mcgreal, and Theodore Sternberg under the supervision of VLRS Director, Dr. Anthony “Jack” Gierzynski and VLRS Deputy Director, Dr. Jonathan “Doc” Bradley in response to a request from Representative Monique Priestley.

Contact: Professor Anthony “Jack” Gierzynski, 517 Old Mill, The University of Vermont, Burlington, VT 05405, phone 802-656-7973, email agierzyn@uvm.edu.

---

[74] California Privacy Protection Agency, *Standardized Regulatory Impact Assessment: California Privacy Protection Agency.*

[75] Ross McKean, John Magee, and Racheal de Souza, “DLA Piper GDPR Fines and Data Breach Survey: January 2025,” *DLP Piper* (January 2025), https://www.dlapiper.com/en/insights/publications/2025/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2025.

[76] Market and Research, *GDPR Services Market Report 2025*, February 2025, https://www.researchandmarkets.com/reports/5820150/gdpr-services-market-report?srsltid=AfmBOopFNwE8IVyGKoJeQZImfTaEXuc-R8HHGCL-_5lrR8rXJPAHHaj3.