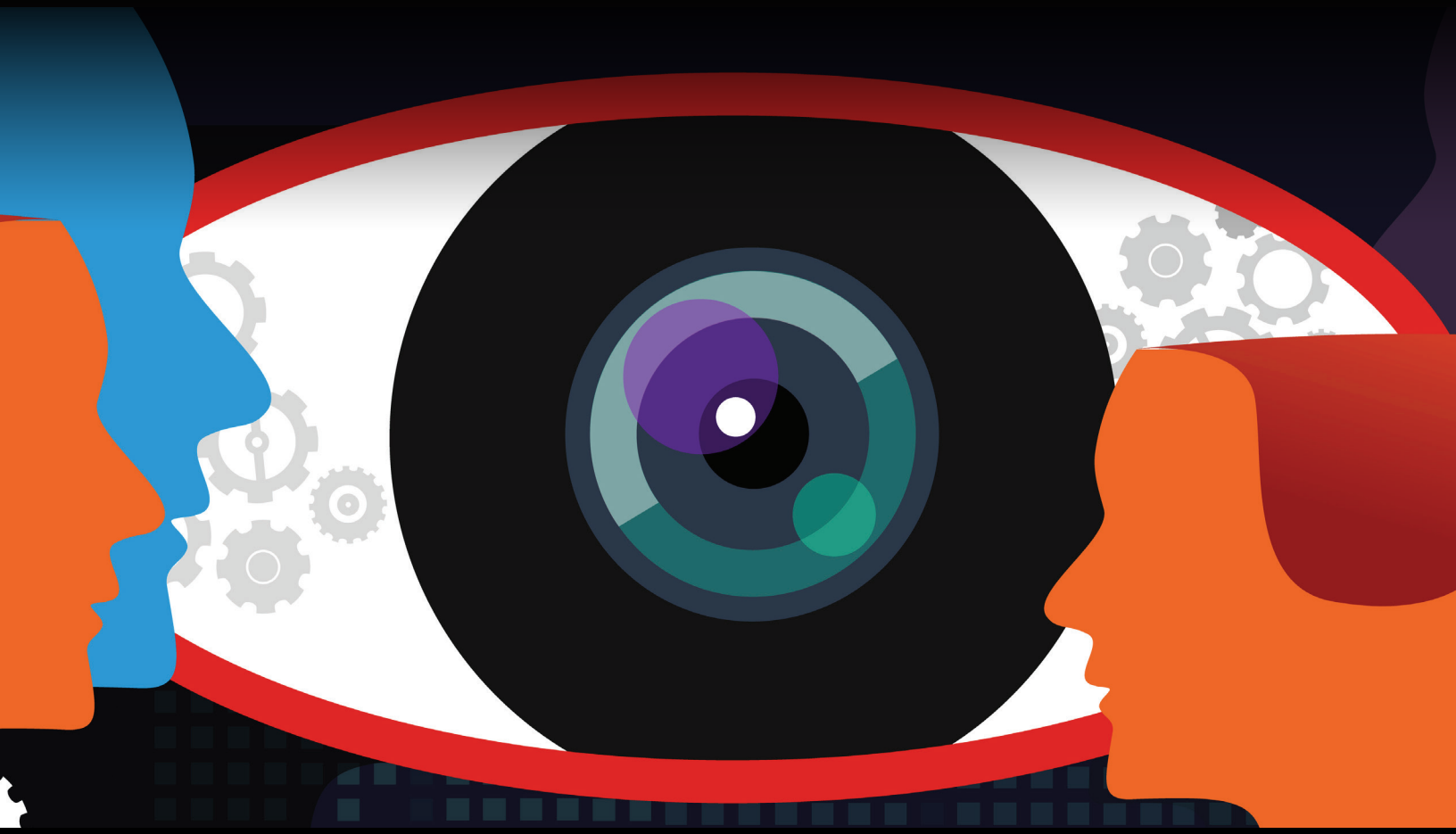
UC BERKELEY

CENTER FOR LONG-TERM CYBERSECURITY



CLTC WHITE PAPER SERIES

Privacy Legislation on the Ground

EFFECTS OF AND RESPONSES TO THE GDPR AND CCPA

SABA CHINIAN

CLTC WHITE PAPER SERIES

Privacy Legislation on the Ground

EFFECTS OF AND RESPONSES TO THE GDPR AND CCPA

SABA CHINIAN

April 2023

CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Contents

Executive Summary

Between 2021 and 2022, the University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC) convened a series of two symposia entitled "Comparing Effects and Responses to the European Union General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA)." The purpose of these convenings was to enable scholars from diverse institutions to share academic research on the effects of two major privacy laws: the GDPR, a European Union (EU) law that came into effect in May 2018 and is uniformly binding in all 27 EU member states, and the CCPA, the first state privacy legislation of its kind in the United States, which entered into force on January 1, 2020 and was later amended by the California Privacy Rights Act (CPRA), which has been operative since January 1, 2023.

The GDPR and CCPA are the most consequential data information regulations since the development of intellectual property law. But from a long-term perspective, the GDPR and CCPA are ultimately "first drafts" in privacy protection.[1] How we conceive of "privacy" and the tools we use to manage it are likely to change. This empirical research on the GDPR and CCPA gives us an opportunity to evaluate these first drafts in order to not only observe their effects on protecting privacy, but also to improve subsequent privacy regulations in the United States and beyond.

Each of the studies presented at the symposia approaches the topic through a different lens — whether by interviewing technology-sector employees and regulators, analyzing compliance processes on different websites and mobile apps, or investigating whether regulators have effectively and consistently enforced the laws. Combined, these papers answer questions regarding how these laws have affected individuals and organizations, whether they have effectively protected data privacy, and how they anticipate the effects of emerging privacy laws. Further, these findings suggest how to better enforce and comply with these laws.[2]

The request for proposals for the symposia asked, "In what areas are the effects of and responses to the GDPR and CCPA converging, and in what areas are they diverging?" The

1 Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019): "The European Union general data protection regulation: what it is and what it means," Information & Communications Technology Law, DOI: 10.1080/13600834.2019.1573501

2 To note, some CLTC Symposium papers have been updated, published, or are near publication. Their updated findings and citations are included in this paper where possible.

research papers presented at the symposia address this inquiry, suggest how to improve compliance, and predict next steps for emerging privacy regulations.

KEY FINDINGS

The GDPR and CCPA introduced new compliance and enforcement mechanisms aimed at protecting data privacy interests. Using empirical evidence from the CLTC Symposium papers, this paper answers specific research questions and shines a light on the effect of these novel and nuanced regulations.

The discussion proceeds in three parts. Section I first explains the achievements of the laws in reaching data privacy goals. To start, the GDPR and CCPA have introduced motivations to encourage corporate compliance that go beyond avoiding regulatory penalties, for example by encouraging firms to limit their reputational risks or improve their ability to integrate into new markets. Large companies seem to have become more wary of introducing new, data-intensive practices following the enactment of both laws. The laws may also be encouraging peer corporate accountability; to avoid liability, companies may want to ensure that the data practices of their corporate clients are compliant before engaging in a transaction. Although enforcement of the CCPA has yet to be fully rolled out and observed, researchers found that the GDPR's enforcement mechanisms have helped maintain accountability and transparency among EU member states.

Section I then delves into the limitations and unintended consequences of the GDPR and CCPA for both companies subject to the laws and for regulators. For companies, vague language and uncertainty in both the GDPR and CCPA have created confusion over what compliance looks like and have led to organizational tension between non-lawyers and lawyers, leading to a risk of unintentional non-compliance. The costliness of compliance with both laws has created barriers to entry for smaller businesses and has incentivized some to cut corners in their compliance strategies. Companies report that complying with the GDPR and CCPA requires difficult, if not impossible, data inventory, mapping, and retention obligations. Additionally, lack of clarity about their obligations for consent interfaces and user-access request processing has increased the risk of noncompliance, harm to user privacy, and abuse.

With regard to enforcement issues, this paper focuses on the GDPR because there has not been enough time to adequately observe complications with enforcing the CCPA. Research presented at the symposia revealed that a lack of resources and expertise among some EU

member states can affect the outcome of their GDPR enforcement actions. And unlike the CCPA, the GDPR's requirements affect individuals and companies of all sizes, which has resulted in disparately heavy enforcement on smaller businesses and individuals. Section I concludes with observations about how the GDPR and CCPA may be affecting innovation and product development, and looks at their impact on startups as well.

Section II puts forward recommendations for how companies can more effectively comply with these laws, and how regulators can better enforce them. For companies, viewing privacy as a business and investment risk can better motivate compliance. Encouraging organizational cohesion, accountability, and transparency can improve compliance and prevent deceptive designs. As for verifying user requests for data, companies can prevent inadvertent leaks to impersonators by requiring multi-factor authentication, notifying the user through other communication channels of the request, or requiring the user to submit verification information.

For regulators, the paper suggests creating safe harbors for small businesses and individuals under the GDPR to prevent excessive punishment. For both laws, clarifying ambiguous language can improve compliance and reduce regulatory uncertainty. Creating more explicit guidelines and enforcement consequences can help eliminate deceptive designs in consent interfaces. Employing a more explicit advisory function to provide guidance and interact with regulated entities or individuals can help prevent infringements from occurring in the first place. In addition, by ensuring that the laws allow companies to share some information with verified researchers, companies can help prevent, address, and remedy infringements.

Section III looks to the future and reflects on how this research on the GDPR and CCPA can inform emerging privacy laws. Following the enactment of the GDPR and CCPA, states across the country have followed suit. Colorado, Connecticut, Virginia, and Utah have all passed statutes concerning data privacy, and nearly 20 other states have active bills. Companies suggest that new laws mirroring the GDPR and CCPA could prevent the havoc of complying with a patchwork of distinct privacy laws. But copying these laws could amplify their negative consequences, and regulators would benefit from learning from the experience of dealing with the GDPR and CCPA to create laws that avoid their pitfalls. Observing the GDPR and CCPA also provides important procedural lessons, such as the amount of time between passage and enactment, for emerging regulations to ensure efficient and effective compliance.

Finally, observing the effects of the GDPR and CCPA can help predict the success of a potential US federal privacy law. A federal privacy law that preempts existing state law could help companies avoid patchwork compliance. But states can operate as "laboratories" of privacy

law that can better react to unforeseen and unintended consequences, such as those resulting from the GDPR and CCPA. Policy experimentation is particularly helpful in this field. Regulating data practices is a novel, complicated, and increasingly important endeavor. Learning from success and failures of existing regulations, such as the GDPR and CCPA, can guide emerging laws towards more effective data privacy protection.

I. Effects and results of the GDPR and CCPA

Research Question: "What are the achievements and/or limitations of the GDPR and CCPA/CPRA in practice, their effect on innovation, and the consequences for how firms and customers re-negotiate their rights and responsibilities around data and data products?"

The studies from the CLTC symposia reflect both successes and limitations of the GDPR and CCPA in protecting customer privacy and holding firms accountable for their data practices. Despite the achievements of these laws, empirical and anecdotal evidence indicates that the GDPR and CCPA have compliance and enforcement shortcomings that interfere with their intended goals. More time may be necessary to gauge the effectiveness of these two new, first-of-their-kind laws, but preliminary findings indicate that stakeholders are still grappling with many of their provisions.

ACHIEVEMENTS

The CLTC Symposium research papers demonstrated that the GDPR and CCPA have effectively signaled to companies the importance of protecting user privacy beyond just the regulatory consequences of noncompliance. As described below, companies may be more hesitant to employ practices or create products that collect or use large amounts of data, particularly when it involves targeting behavioral advertising, because of the risks of violation. This avoidance of risky practices may also increase corporate peer accountability due to the interconnectedness of technology companies. Companies may be motivated to ensure that their corporate clients or vendors are compliant, or entirely avoid those with risky data practices, to avoid liability or reputational harm. Enforcement of the CCPA has yet to be fully researched, but the GDPR employs enforcement mechanisms that can promote transparency, accountability, and consistent enforcement across the EU. For instance, the regulation's arbitration mitigation mechanism allows EU member states to object to and effectively "appeal" each other's decisions. The GDPR also allows NGOs to raise alarm bells regarding infringements and hold EU member states accountable to handling violations.

More than just a regulatory risk

Both the GDPR and CCPA impose fines and penalties to not only punish infringing companies, but also deter noncompliance by introducing new types of risks. The first is financial, as both laws impose penalties for violations. Violating the GDPR could result in a fine of 20 million Euros or four percent of total worldwide annual revenue, whichever is greater, while violations of the CCPA may result in up to $7,500 per violation. Companies take these consequences seriously. Wong et al. explored the Securities and Exchange Commission (SEC) filings of nine major technology companies to analyze how they interpret and translate the GDPR and CCPA as different types of business risks to investors.[3] According to this research, DoorDash, Google, Microsoft, and Uber all explicitly mentioned the financial penalties for violations of the GDPR or the CCPA in their SEC filings.[4] Shareholders could make the GDPR and CCPA the basis of a shareholder liability suit, deterring large companies from risking noncompliance. Through their SEC filings, managers of these companies are telling investors that they cannot perform their duty of wealth maximization of business assets because some activities are simply too risky now from a regulatory perspective. Thus, investors cannot sue managers for "waste" for not taking ultra-radical personal data approaches.

Investment risks are not limited to large companies. Anđelković and Šapić examined how Serbian startups interpret and comply with the GDPR and CCPA.[5] Their survey and interviews showed how the GDPR has achieved some success in gaining compliance from these smaller companies. The surveys indicated that a majority of startups perceive GDPR compliance as heavily related to the interests of investors (13 out of 19 respondents).[6] The GDPR became a part of the organizational structure of many of these startups, with the majority having someone in their firm responsible for GDPR compliance (10 out of 19 respondents).[7] Startups prioritized compliance with the GDPR because of costs — not those associated with fines, but instead, the cost of losing investments.[8] The startups anticipated lower or withdrawn investments for not being compliant with the GDPR.

3 Wong, Richard Y., Andrew Chong, and R. Cooper Aspegren. "Privacy Legislation as Business Risks: How GDPR and CCPA Are Represented in Technology Companies' Investment Risk Disclosures." Proceedings of the ACM on Human-Computer Interaction, Article 82, 7, no. CSCW1 (April 2023). https://doi.org/https://doi.org/10.1145/3579515. Available currently at: https://escholarship.org/uc/item/9mh2h52k, 2.

4 Wong, 10

5 Branka Anđelković and Jelena Šapić, "Alice in Wonderland: Challenges of Data Compliance for Startups - The Case of Serbia." 2022 CLTC Symposium, 1.

6 Anđelković, 21.

7 Anđelković, 20.

8 Anđelković, 23.

Companies are also concerned about how violating the law creates reputational risk: Microsoft, Google, Facebook, and Salesforce all added new language in their SEC filings warning that violating GDPR and CCPA could hurt their reputation and brand.[9] The laws also affect internal business practices in ways that may indirectly benefit user data privacy. Facebook reported that its advertising revenue experienced a downturn following the passage of the GDPR, suggesting that its targeted behavioral advertising practices had suffered.[10] Airbnb and Facebook reported that the ability of users to opt-out of marketing cookies reduces their ability to market and advertise their products.[11] This suggests that the laws' efforts to limit the use of personalized data in targeted advertising have been successful.

Not complying with the privacy laws curtails business opportunities. Startups competing to gain market advantages are incentivized to comply with the GDPR and CCPA to gain access to lucrative geographic regions. The GDPR's harmonization of separate data privacy regulations across the EU mean that by complying with just one set of standards, startups have access to the entire EU market.[12] While the startups that emerged after the GDPR's passage had already integrated GDPR compliance, the startups that existed before the GDPR found that it actually expanded their potential reach. In fact, the cost of compliance, even for a small company with limited resources, was outweighed by the attractiveness of the EU market. The same was true for CCPA compliance, which startups felt was a "necessary step for doing business in hyper-connected and globalized markets."[13]

Potentially deterring data-intensive practices and increasing peer corporate accountability

Research presented at the CLTC symposia also highlighted how the GDPR and CCPA have potentially limited the use of targeted behavioral advertising and the creation of data-intensive products, in line with privacy regulators' goals. In SEC filings from 2015, both Microsoft and Google noted that their increase in web- and cloud-based products would collect more personal data, leading to greater risk for privacy and data protection breaches that could result in legal liability or reputational harm. Three years later, Microsoft and Salesforce included a new risk factor regarding ethical risks associated with creating AI systems and the potential for

9 Wong, 10–11.
10 Wong, 11.
11 Wong, 13–14.
12 Anđelković, 25.
13 Anđelković, 15.

reputational harm.[14] The research also indicates the GDPR and CCPA provisions limiting the use of targeted behavioral advertising have been effective, as demonstrated by the decrease in these large companies' advertising revenue and marketing capabilities. Facebook, which reported that it earns 97 percent of its total revenue from advertising, stated that the GDPR and CCPA had limited the "ability to target and measure the effectiveness of ads on our platform, and negatively impacted our advertising revenue." Still, while companies might recognize the risk of developing AI products and their targeted advertising practices may have decreased, their SEC filings do not necessarily indicate that the creation of new data intensive products is slowing down.

These privacy laws may also be encouraging peer accountability to reduce the aforementioned risks of noncompliance. Large companies must also hold their business clients and companies they rely on accountable to these privacy laws to avoid liability themselves. Salesforce noted that its compliance with the GDPR and CCPA extended to its enterprise clients, and that it needs to provide clients with education regarding privacy and data protection compliance during the sales process. This could take up more time and resources and could deter the company from engaging with riskier enterprise clients entirely.[15] Furthermore, large companies often rely on each other to support their products or for advertising, which means they must look to ensure that their peers are in accord with the GDPR and CCPA to avoid risk of noncompliance. Airbnb, Doordash, Facebook, and Uber reported that they are dependent on Apple's and Google's mobile operating systems and platforms for their mobile applications. Changes made by Google or Apple to their data collection, such as making it more difficult to track and advertise to users, directly affect the data practices of such mobile apps.[16] The interconnectedness of these stakeholders on each other's privacy practices implies that these laws could create a ripple effect that leads large tech companies to be accountable to each other.

Of course, the SEC filings are limited insofar as they only *anticipate* increased peer accountability based on how companies signal to investors the risks of clients' or other businesses' privacy infringements. Still, companies feel obligated to signal to investors the potential risks and costs of these privacy laws to their data-heavy practices and policies, which could result in less investment (and thus less product development) in those areas.

14 Wong, 12.
15 Wong, 13.
16 Wong, 13-14.

Effective transnational enforcement

In their research on enforcement of privacy laws, Li and Newman found that the GDPR's mechanism for mitigating arbitration has increased company accountability and consistent enforcement across the European member states.[17] This mechanism has increased horizontal accountability by allowing peer regulators to raise objections to and attempt to alter enforcement actions, and has improved vertical accountability by allowing civil society actors, such as NGOs, to "name and shame" lax enforcement and rally public pressure. This supranational institutional procedure mitigates inconsistent application of the GDPR across member states.

The arbitration mitigation mechanism is made up of primarily two articles: Article 60 and Article 63. Article 60 minimizes overlapping enforcement suits by determining how national data protection authorities should cooperate and coordinate their enforcement actions for cross-border cases —specifically, by creating what's been referred to as a "One-Stop-Shop." Under this system, firms receive primary oversight by a lead supervisory authority (LSA) in the country where they are mainly established in the EU. For cases that have a cross-border dimension, Article 60 identifies a LSA and requires cooperation with other concerned supervisory authorities (CSAs). If all these supervisory authorities reach a consensus, then a decision is adopted. If the LSA does not resolve objections, it must submit the matter to the consistency mechanism, explained under Article 63. Under Article 63, the LSA first refers cross-border cases that cannot reach a consensus to the European Data Protection Board (EDPB) for a binding decision. Article 63 also allows the EDPB to issue opinions on matters that affect more than one member state. The flow chart in Figure 1 reflects this mechanism.

Consensus-based decision-making processes in cross-border GDPR cases boosts horizontal accountability. At the end of 2019, 79 of the 141 draft decisions submitted through the One-Stop-Shop were finalized, and all reached consensus without requiring dispute settlement by the EDPB. Information sharing is also strong under the GDPR; in the GDPR's first year, 79.5 percent of mutual assistance requests from supervisory authorities were answered within 23 days. Through November 2020, there were a total of 116 Article 60 final decisions and an average of six concerned supervisory authorities for each case.

17 Li, Siyao, and Abraham L. Newman. "Over the Shoulder Enforcement in European Regulatory Networks: The Role of Arbitrage Mitigation Mechanisms in the General Data Protection Regulation." *Journal of European Public Policy* 29, no. 10 (2022): 1698–1720. https://doi.org/10.1080/13501763.2022.2069845, 1.

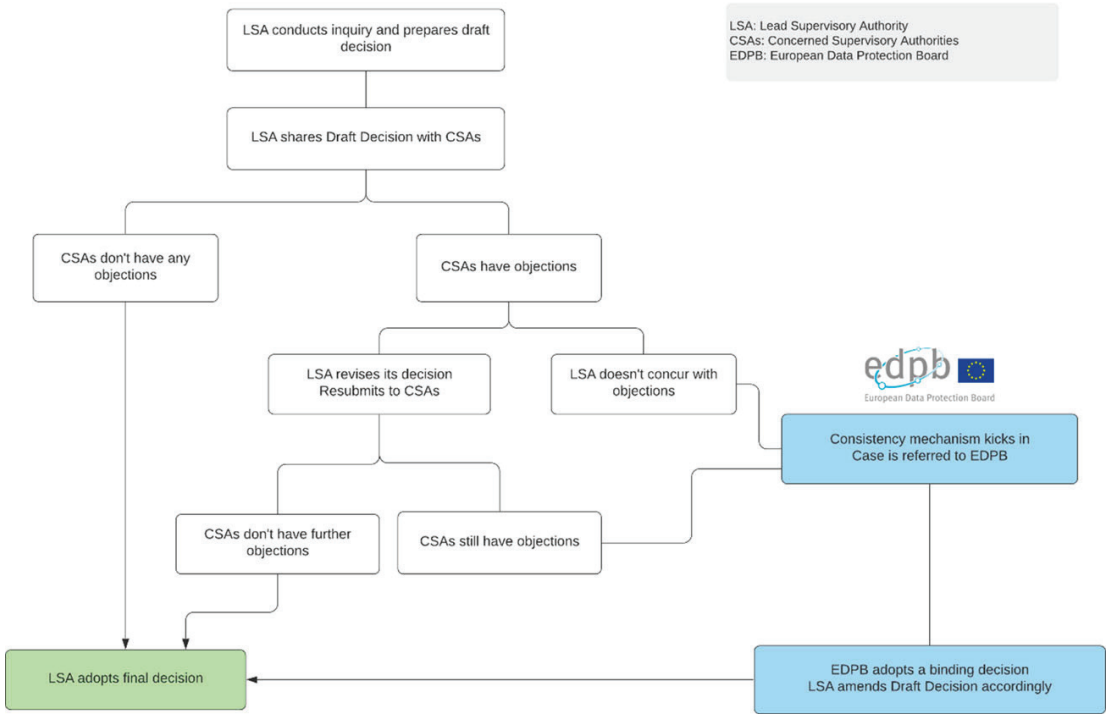


Figure 1: How a cross-border GDPR case reaches a final decision.[18]

As the Li and Newman study notes, many criticize the One-Stop-Shop system for concentrating cases in Ireland and Luxembourg, which have relatively small regulatory agencies compared to those in larger member states. Ireland, in particular, has attracted technology companies because of its low corporate income tax and reputation for light-handed enforcement of data privacy laws, which some perceive as a "loophole" for compliance.[19] This concentration of cases in Ireland and Luxembourg could imbalance enforcement by siphoning investigations to where companies are located, creating different levels of power among the EU member states' Data Protection Authorities (DPAs).[20]

18 Li, 9.

19 Li, 2; Hoofnagle, Chris Jay, Bart van der Sloot & Frederik Zuiderveen Borgesius (2019): The European Union general data protection regulation: what it is and what it means, Information & Communications Technology Law, DOI: 10.1080/13600834.2019.1573501, 71.

20 Sivan-Sevilla, Ido. "Varieties of Enforcement Strategies Post-GDPR: A Fuzzy-Set Qualitative Comparative Analysis (FSQCA) across Data Protection Authorities." *Journal of European Public Policy*, 2022, 1–34. https://doi.org/10.1080/13501763.2022.2147578, 8–9.

Still, Li and Newman suggest that the small size of these nations or their interest in attracting tech companies ultimately does not reduce enforcement because other DPAs can hold them accountable. Two cases in Ireland — one with Twitter and the other with WhatsApp — show how the GDPR's mechanisms can prevent underenforcement and level the regulatory landscape across jurisdictions. For example, Twitter users suffered a personal data breach in 2019 and delayed notifying Irish authorities. Ireland issued an opinion that Twitter had failed to notify authorities of the breach within 72 hours. Several CSAs raised objections under Article 60 that Ireland's opinion was inadequate because Twitter had infringed additional provisions of the GDPR. After Ireland responded to the objecting member states, most maintained their objections and Ireland referred the matter to the EDPB dispute resolution procedures. The result was a binding decision by the EDPB for a 450,000 euro fine against Twitter.[21]

In 2018, Ireland had investigated WhatsApp for violations of its transparency obligations under GDPR Articles 12–14, specifically for failing to give users enough information on how it shared personal data with its parent company, Facebook. Ireland drafted a decision to impose a penalty of 30–50 million euros. Eight CSAs objected to the scope of the infringement and proposed remedies. Ireland refused to implement the suggested edits, consensus was not reached, and the case was forwarded to the EDPB dispute resolution process. The EDPB amended Ireland's draft decision to align with the objections of the CSAs, ultimately fining WhatsApp 225 million euros.[22]

These GDPR accountability measures have also held Luxembourg's enforcement accountable. After investigating Amazon for carrying out targeted advertising systems without proper user consent, Luxembourg gave an initial opinion regarding Amazon's infringements and the fine amount. After feedback from CSAs, and without even requiring the dispute settlement procedure, Luxembourg nearly doubled Amazon's fine, ultimately resulting in a record-breaking 746 million euro fine. These cases demonstrate how powerful the objections from member states are, and how the GDPR's arbitration mitigation mechanisms promote transparency and consistent enforcement across the EU.[23]

The GDPR's support of the role of NGOs in ringing the alarm about potential violations also increases accountability and public awareness. National regulatory bodies, such as DPAs, have

21 Li, 10–11.
22 Li, 11–12.
23 Li, 12.

limited reach and resources to detect violations.[24] Article 80 allows NGOs to bring complaints and garner attention for potential data breaches and misuse. These NGOs decentralize the monitoring systems across member states and offset information asymmetries between citizens, regulators, and companies. They can also inform and mobilize society through press releases and campaigns that keep regulators motivated and accountable. And they can bridge cross-border violations and bring complaints against firms across multiple member states.[25] Decentralized actions brought by NGOs have resulted in significant penalties: one French-based NGO, Noyb, collected over 9,000 participants to bring an Article 80 action against Google, resulting in a record-breaking 50 million euro fine in 2018.

LIMITATIONS

Despite the success and potential benefit of the GDPR and CCPA, most studies (including those that presented the laws' achievements) found several issues with how companies have tried to comply with these laws, and how regulators have enforced them. Companies have struggled to interpret and apply the requirements of the GDPR and CCPA, and those that lack financial or technical resources can become unavoidably non-compliant. These vague compliance requirements have also created organizational tensions and given rise to risks of abuse. Research on enforcement, currently limited to that of the GDPR, reveals how a lack of resources and expertise can affect enforcement actions, and how the GDPR's large scope can impose disparate enforcement on small companies and individuals.

Issues with compliance

The GDPR and CCPA were among the first data privacy regulations, and many companies subject to their regulation have struggled to understand the laws and ultimately comply with them. As described below, empirical research has identified several reasons why companies are struggling to comply with these laws and the risks of harm that could result from this uncertainty.

24 Jang, Woojeong, and Abraham L. Newman. "Enforcing European Privacy Regulations from below: Transnational Fire Alarms and the General Data Protection Regulation." *JCMS: Journal of Common Market Studies* 60, no. 2 (2021): 283–300. https://doi.org/10.1111/jcms.13215, 289.

25 Jang, 284.

Vague language

Regulators may have wanted to keep language in the GDPR and CCPA more open to give flexibility to companies to comply and grant themselves the ability to apply privacy regulation to ever-changing technologies, but ambiguous language can end up doing more harm than good and backfire in unexpected ways. For instance, vague language in the GDPR has disproportionately targeted smaller entities and individuals, particularly those from marginalized communities. In a study, Mary Fan analyzed 571 GDPR penalty decisions from 20 nations in the EU and found that enforcing privacy laws can, in fact, harm civil liberties and cover up harassment against disfavored groups.[26] Fan's article sheds light on the potential and actual risks that can result from overly broad and ambiguous regulations. The GDPR does not penalize only large tech companies, but also individuals and small businesses, which can be targeted and penalized for up to 20 million euros (approximately US $23.5 million) or, for a business, up to four percent of total global annual revenues, whichever is higher.

EU member states also have the power to add more penalties that are "effective, proportionate and dissuasive" — language that is as ambiguous as it is harmful. The dangers of such a penalty system came to light when a Turkish kebab stand owner and employee attempted to stop xenophobic and racist police harassment they experienced at their shop in Vienna. The owner and employee installed a surveillance camera to record the harassment, which the officer reported to the DPA. They were criminally convicted with violating the GDPR and were given the option of paying a 1,500 euro fine (about $1,771) or serving a four-day custodial sentence.[27]

Fan specifically notes the broad and encroaching power of GDPR Article 5, which lays out a broad statement of principles, including fair and transparent data processing, and adequate, relevant data collection limited to what is necessary and relevant. In one example, a low-income Hungarian national in Austria had a motion-triggered dashcam that he used to record accidents. After it was discovered by police during a roadside stop, they put him in criminal proceedings for violating Article 5 and Article 6, which concern the lawful processing of data and requirement of subject consent. The Austrian DPA ruled that the dashcam was a "systematic violation" of the GDPR and refused to recognize any "legitimate interest" in the operation of the dash cameras.[28] The driver, a father of three children, one of whom was

26 Fan, Mary. "The Hidden Harms of Privacy Penalties." *UC Davis Law Review* 56 (June 24, 2022). Available at SSRN: https://ssrn.com/abstract=4143821 or http://dx.doi.org/10.2139/ssrn.4143821, 6.

27 Fan, 6.

28 Fan, 35.

physically disabled, earned a monthly income of 900 euros and was 1,300 euros in debt. The Austrian DPA imposed a fine of 300 euros, or 30 hours of substitute imprisonment.

This was not an isolated incident. In her investigation, Fan collected privacy penalty decisions from 20 European Member States between 2018 (when the GDPR first came into full effect) through January 3, 2022.[29] Fan's research revealed that small businesses comprised 15.5 percent of the targets penalized by these Member States. Individual targets made up nearly six percent of the targets, nearly half of which involved disputes between neighbors.[30]

The most prevalent grounds for penalties against individuals were under GDPR Article 5 (70.6 percent) and Article 6 (61.8 percent).[31] Articles 5 and 6 accounted for a significantly larger proportion of penalties against individuals than against major corporations.[32] Article 5 requires that personal data be processed in a manner that is "adequate, relevant, and limited," "fair," and "transparent." Article 6, the second most prevalent basis of penalties against individuals, requires consent by the data subject for processing, unless an exception applies, such as the "vital interests of the data subject or another person" or necessity to perform a contract.

For penalties against small business, the two most prevalent bases were under Article 5 (52.2 percent) and Article 13 (38.9 percent). GDPR Article 13 governs notice and the information a data controller must give to the subject when personal data is collected. For her research sample, Fan's analysis found that GDPR Articles 5 and 13 accounted for a larger proportion of privacy penalties against small businesses than major corporations.[33]

Large companies were most commonly subjected to penalties under Articles 7 and 32.[34] Article 7 governs the conditions for obtaining and demonstrating consent for processing data, and prescribes the right to withdraw consent. Article 32 requires controllers and processors to "implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk," including, among other measures, "pseudonymisation and encryption of personal data" and "resilient" processing systems and services. Article 7 was significantly more likely to be the basis of penalties against major corporations than small businesses, and

29 Fan, 28.
30 Fan, 28.
31 Fan, 32, Table 5.
32 Fan, 32, Table 6.
33 Fan, 33.
34 Fan, 34.

Article 32 was significantly more likely to be the basis of penalties against major corporations than either individuals or small businesses.

Fan argues that the differences in GDPR Articles used against individuals and small businesses, compared to those used against large companies, are due to vague language. Individuals and small companies are less savvy about the law than major companies, and do not have the same vast resources to parse unclear legal language and defend themselves. For example, Article 5 — the most prevalent basis for penalties against individuals and small business — does not provide clear definitions for what counts as "adequate, relevant and limited" and "fair" data collection. Fan argues that these ambiguous standards do not give enough notice to individuals or small businesses related to how to comply in advance and prevent infringement. Rather, it allows for selective, even discriminatory *post hoc* punishment based on malleable standards.[35] Meanwhile, the GDPR provisions that are most likely to subject large companies to fines are more specific, such as Article 32, which includes specific examples and guidance on compliance.[36]

Vague language also decreases the organizational cohesion and productiveness of small- and medium-sized businesses in interpreting and complying with the GDPR and CCPA. Kwong's paper focuses on small- and medium-sized enterprises (SMEs) and how the ambiguity of privacy laws created tensions between internal departments that have competing interests.[37] Between 2020 and 2022, Kwong conducted 18 interviews with law, privacy, and security experts from various sectors (including education, healthcare, business, and advertising) and asked how practitioners balance compliance with their normal operations.[38] Participants described that compliance was complicated by misconceptions around privacy expectations, unstable regulatory environments, and difficulty deciphering laws in practice. Specifically, the inconsistent standards among the patchwork of existing privacy laws created confusion about how organizations were expected to respond, particularly in industries without previous experience with such regulations.[39]

In many firms, the ambiguity and unpredictability regarding GDPR and CCPA regulation created internal resistance to change and tension between departments.[40] In fact, interviewees

35 Fan, 43.

36 Fan, 44.

37 Kwong, Jillian. "Translating Data Protection into Practice: Exploring Gaps in Data Privacy and Regulation within Organizations." 2022 CLTC Symposium, 10.

38 Kwong, 11.

39 Kwong, 20.

40 Kwong, 15.

unanimously agreed that one factor disproportionately complicated their internal compliance processes: imprecise definitions within data privacy laws.[41] The laws provided little guidance in interpreting vague terms, leading to multiple interpretations and allowing for definitions to be molded based on the priority of the department.[42] Competing interpretations results in disorganized and uncertain compliance practices, and accountability metrics were often shortcut.

Vague regulations can not only result in unintentional noncompliance, but can create loopholes that can be abused by stakeholders. Legal strategists have interpreted the "legitimate interest" legal basis to justify a laundry list of data uses, in effect warping the GDPR to allow any use of data.[43] For their study, Kyi et al. analyzed how the vague "legitimate interest" standard in the GDPR is misused, resulting in deceptive designs.[44] The GDPR lays out six grounds for legally processing data, the last of which is processing done in the "legitimate interests" of the data controller or third parties. "Legitimate interest" is not explicitly defined in the GDPR, but is satisfied when the "interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."[45] Although not stated explicitly in the GDPR, experts have suggested that this provision indicates that "legitimate interest" is considered satisfied by a three-part test: (1) *purpose*, requiring that companies have a purpose behind the legitimate interest; (2) *necessity*, meaning that processing is necessary to serve the legitimate interest, and (3) *balancing*, meaning the legitimate interest does not override the individual's interests, rights, and freedoms.[46]

This derivative test allows for broad interpretations and flexible use of user data, without requiring user consent. This vagueness can permit the use of deceptive designs, which are user interfaces that "trick" users to make decisions that benefit the online service. In the GDPR context, this might be a website that manipulates users into clicking "Accept all cookies" by highlighting that button while hiding the "Reject all cookies" button. It could also entail the use of overly technical language to deceive users into consenting, or generously interpreting

41 Kwong, 23.

42 Kwong, 24.

43 See e.g. Hunton & Williams LLP, Centre for Information Policy Leadership GDPR Implementation Project, 'Recommendations for Implementing Transparency, Consent and Legitimate Interest under the GDPR,' 19 May 2017.

44 Kyi, Lin, Asia Biega, and Franziska Roesner, "Investigating Dark Patterns in GDPR's Legitimate Interest." 2022 CLTC Symposium, 1.

45 GDPR, Recital 47.

46 "What Is the 'Legitimate Interests' Basis?" Information Commissioner's Office. Accessed December 17, 2022. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#article_61f.

"legitimate interest" to be broader than is allowed to not require consent at all. But there is little to no deterrent for using these deceptive designs because of the lack of regulatory oversight or punishment of such practices.[47]

To analyze whether and how often "legitimate interest" is used in deceptive designs, Kyi et al. used a web crawler to collect data from 10,000 websites and quantify the frequency of the term "legitimate interest," and then used qualitative analysis to assess the presence of elaborate deceptive designs.[48] Of the 10,000 websites, 474 websites included "legitimate interest" in their consent notices.

The researchers found that almost every website with "legitimate interest" in its consent banner mentions opt-out language for legitimate interest, but not every website allows users to opt-out.[49] Those that allowed opt-out often complicated the process by either requiring users to opt-out of each legitimate interest purpose individually, or by requiring users to go through vendors to opt-out. Legitimate interest was often automatically selected, requiring users to opt-out manually. This is particularly problematic because personalized advertising was often listed as a "legitimate interest" purpose.[50] Because of the vague and broad allowances of "legitimate interest" under the GDPR, firms can continue to unintentionally or intentionally deceive users and misuse their data without consequence.

Smaller companies that are compliant with the GDPR also note the risk of "legitimate interest" allowing for loopholes, but for them, the broad definition exposes them to operational risks.[51] The vagueness of the definition undermines the ability of intellectual property owners to enforce their rights against alleged infringers because they need to show a legitimate interest to get access to the infringers' details.

Organizational issues

"*There has not been any certainty. There has not been any stability over what this law ultimately looks like and that remains true right now* [*July 2020*]. . . . *So when a company is trying to figure what they need to do and when that answer has not been incredibly easy to come by there's a lot of uncertainty and it puts lawyers, in particular, in a position of having to not be certain, which is what people hate*

47 Kyi, 6.
48 Kyi, 7.
49 Kyi, 10.
50 Kyi, 10.
51 Anđelković, 17.

about lawyers. We always say 'it depends' or 'this is defensible' or whatever and there's no kind of ultimate certainty around this and that's still the case." — Privacy and data security lawyer.[52]

Beyond a lack of clarity in language, Kwong's paper delved into how SMEs struggled with approaching uncertainty and infeasibility. Over half of the interview participants noted that unpredictable conditions made it difficult to advance privacy within an organization. Feasibility was also an issue: leadership was skeptical about devoting large amounts of resources to build practices around mandates that were still up in the air. This led to what was a perceived "regulatory limbo."[53] A large part of the challenge with communicating internally about data privacy is its abstract nature. Unlike cybersecurity, threats to privacy were not fully understood within most organizations when the GDPR and CCPA were enacted. This lack of internal knowledge and cohesion, coupled with infeasibility and uncertainty, led stakeholders away from the comprehensive, long-term data protection processes that regulators envisioned. Companies that conduct business outside the US indicated in their interviews that they would consider a more comprehensive option in order to comply with global data sharing and transfer regulations, but it was often perceived as unnecessarily expensive, and not worth the cost of disrupting business operations. Instead, stakeholders (particularly those without global data sharing processes) reported that they often opted for "short-term, minimally intrusive, low commitment 'fixes' that allowed their organizations to demonstrate compliance without disrupting normal operations or costing too much money."[54] Furthermore, stakeholders with pre-existing data protection systems were unwilling to overhaul their infrastructures to meet uncertain regulatory standards. Leadership did not prioritize data privacy or integrate it into regular business decisions, which often led to cutting corners and disorganized compliance policies. At the same time, embracing privacy goals had the risk of backfiring if companies failed to meet their promises, leading to more mistrust and scrutiny.[55]

Privacy laws often subjected companies to tensions specifically between lawyers and tech workers. Elliot and Susan Kennedy conducted interviews with five designers and front-end developers with experience creating cookie banners for implementing GDPR regulations.[56] The interviews revealed that discussions about compliance usually center on legal text, rather than interactive visual elements, and that preference is given to compliance with laws over the usability of the consent feature. Lawyers preferred denser text, leading to complicated, con-

52 Kwong, 19.
53 Kwong, 19.
54 Kwong, 31.
55 Kwong, 34.
56 Elliott, Ame and Susan Kennedy. "From Policy to Pixels: Strategic UX Design Support for GDPR Implementation." 2022 CLTC Symposium, 10.

fusing language that obstructed user-friendly cookie banners. But the usability and clarity of the cookie banner is precisely the point, as it aims to give users a clear understanding of what they are consenting to. Sacrificing usability for strict compliance was a common, if hypocritical practice. As noted by Elliot et al. and as researched by Kyi, deceptive designs can emerge when cookie banner language is complicated or too long.[57] Dense language can trick users into opting in, and complicated legalese can deter them from wanting to read through the banner and lead them to opt-out for their own convenience.

In interviews with tech workers across engineering, product, design, user research, and compliance/operations groups, Grover found that this tension could result in tech workers resisting working with lawyers. One senior engineer at a large technology conglomerate described their team's reluctance to consult lawyers about whether a third-party service was compliant because "it usually ended up being more work."[58] Several other participants stated that legal expertise was unavailable, either by design or because of lack of capacity. One participant stated, "The struggle was that nobody wanted to talk to a lawyer to give us any understanding of the things we should do. . . . It was something that . . . felt like it was actively being avoided. . . ."[59]

Where legal advice was lacking, compliance was often led by non-lawyer tech employees, which led to limited accountability, responsibility, and effective compliance.[60] Grover found that tech workers often navigated uncertain compliance policies with limited capabilities, but remained autonomous. They reported high levels of authority with minimal oversight, which led to a lack of accountability. One developer stated that their process of identifying risks with third-parties was not overseen, and "we could have easily flaunted it entirely and nobody would have known; nobody was in a position to question us."[61] Developers perceive compliance work as a "one-time" project, and all participants admitted that they had not returned to the processes to ensure quality or to audit them. Instead, they would wait for bugs, which were rare because users are unlikely to notice or complain if their privacy preferences, such as cookie consent settings, do not work properly. In fact, several participants described bugs in their initial implementations of cookie consent notices and opt-ins, but none of the participants reviewed that work. The studies together demonstrate that, with or without lawyers, engineers are uncertain and grappling with the expectations and responsibilities imposed by privacy regulations.

57 Elliot, 3; Kyi, 6.
58 Grover, Rover. "Encoding Privacy? How Tech Workers Shape Privacy Regulations." 2022 CLTC Symposium, 1.
59 Grover, 10.
60 Grover, 1.
61 Grover, 10.

Delegating compliance outside of the organization poses a series of challenges, as well. As noted by Elliot et al., consent management providers such as One Trust, QuantCast, and Cookiebot provide customizable templates for data protection policy compliance across multiple jurisdictions. But they are often too complicated, and can often incentivize illegal practices.[62] Open source code options can provide a more cost-friendly alternative, but require people to have sufficient technical skills to implement them. Plug-in compliance solutions, like those available for WordPress-based websites, are not easily accessible for those with lower technical skills or financial resources.[63]

Technical issues

Several papers touched on issues that arose as firms worked to comply with the technical requirements of the GDPR and CCPA, such as consent interfaces and verifiable consumer requests for data. As mentioned in studies by Kyi and Elliot et al., deceptive designs in consent interfaces can emerge as a result of vague language and organizational tensions between compliance and user-friendliness.[64] Through a study of 50 business websites in California and Europe, Mahoney found limited protections against targeted advertising and a blurred line between opt-in and opt-out language in consent due to deceptive designs with cookie consent dialogue and legitimate interest loopholes.[65] Consent interfaces required consumers to toggle through complicated pop-ups in order to opt-out of advertising cookies. Some websites provided the option to refuse cookies and exit in smaller text than the option to accept, and hid it in the corner of the pop-op, while the option to accept cookies was highlighted and in plain sight.[66] Other consent pop-ups would not provide a clear option to reject at all; the option to do so was embedded in something like "Cookie Settings" or "Show Purpose." Only there could consumers opt-out, although it is not obvious that clicking those options would allow them to do so.[67]

Furthermore, a majority of both European (68 percent) and Californian (80 percent) websites researched directed consumers to third-party sites to opt-out of third-party ads or cookies, a step that consumers are unlikely to take to effectively disallow the use of their data for targeted advertising.[68] In Europe, 36 percent of the websites analyzed claimed that personalized

62 Elliot, 11.
63 Elliot, 14.
64 Elliot, 3; Kyi, 6.
65 Mahoney, Maureen. "Beyond Opt In and Opt Out: Publisher and Advertiser Approaches to Targeted Advertising." 2021 CLTC Symposium, 5–6.
66 Mahoney, 10–11.
67 Mahoney, 13.
68 Mahoney, 15–16.

advertising was a legitimate use of data under the GDPR and so did not require prior consent, requiring consumers to take more steps to order to stop tracking. For example, users would have to click on the option to manage cookies, then search for the data use purpose to disable personalized ads and content.[69] Mahoney emphasized how this research reflects the strong financial incentives that companies have to continue their marketing, despite regulatory intervention.[70]

The complicated nature of data tracking and uncertainty around consent interface requirements under the GDPR and CCPA protects these deceptive designs.[71] Considering that regulators enacted the GDPR and CCPA in part to limit the power of websites to use personal data for advertising purposes without user consent, in practice, that goal seems far from achieved. These laws intended to make it easy for consumers to exercise their privacy preferences, but confusing, arduous, and misleading consent interfaces show how these regulations have fallen short.

As for consumer requests for data, research by Samarin et al. found that many phone apps fail to comply with the CCPA's requirements for verifying and processing a verifiable consumer request (VCR).[72] Of the 160 different apps analyzed, the researchers found that only 109 apps included CCPA-specific disclosures in their privacy policies. Of these 109 apps, only 80 were responsive or successfully verified the consumer's identity. Of these 80, 69 (63 percent) provided data in response to the request — but only nine of the apps fully disclosed the extent of their data collection practices.[73] Eight apps (seven percent) replied that they held no data for the consumer, but the researchers found that seven of those apps actually did collect data across a range of CCPA-defined categories of personal information, including identifiers, geolocation data, and sensory data.[74] The remaining three apps redirected consumers to receive the requested information directly from their account profiles.

The CCPA's "right to know" provision also enumerates the type of information that must be provided in response to a VCR. The information provided by the 69 responsive apps varied greatly in their compliance with this provision. Only 24 companies (35 percent) provided

69 Mahoney, 14.
70 Mahoney, 2
71 Mahoney, 6; Kyi, 6.
72 Samarin, N., Kothari, S., Siyed, Z., Bjorkman, O., Yuan, R., Wijesekera, P., Alomar, N., Fischer, J., Hoofnagle, C. and Egelman, S., 2023. Measuring the Compliance of Android App Developers with the California Consumer Privacy Act (CCPA). In The 23rd Proceedings on Privacy Enhancing Technologies, Vol. 3, 2–3.
73 Samarin, 8.
74 Samarin, 9–10.

the categories of personal information collected, 18 (26 percent) provided the categories of personal information disclosed or sold to a third party, 25 (36 percent) provided the categories of those third parties, 30 (43 percent) responded with the business or commercial purpose for collecting or selling personal information, and 23 (21 percent) disclosed the sources from which the information was collected.[75] Furthermore, the CCPA describes steps to verify the identity of the data subject submitting the VCR to prevent the inadvertent disclosure of personal information to someone impersonating the consumer. Many of the apps examined did not use any identity verification mechanism beyond a proof of access to the email account.[76]

Privacy laws require that companies understand how data goes into and out of their systems, but data inventory can be difficult, if not impossible, to compile. Kwong's interviews reflected that many companies often knew little about their data feeds.[77] Interviewees noted that the two methods for data mapping — surveys and automated solutions — were both unreliable and complicated. Surveys, the most common strategy for data mapping, involved distributing standardized surveys internally to identify stakeholders who came into contact with data in every business unit of the company. This is a labor-intensive, complex process that requires unreliable self-reporting. Meanwhile, automated solutions rely on AI or scanning technologies, but large upfront costs make this more cost-prohibitive, and automated solutions were seen as less reliable than surveys because they did not get as much input and did not identify workarounds or actions that fell outside documented practices. The process is also time-intensive: a fairly comprehensive inventory mapping could take up to six months. Despite noting the importance of data inventories, participants emphasized that time and resource constraints put pressure on them to speed up the process even if it resulted in lower quality results. Data retention requirements were also difficult for companies to reach because, prior to the GDPR's enactment in 2018, there was no precedent for deleting unused data. The amount of data being generated and collected daily, combined with ever-changing regulations and expectations, made it nearly impossible for companies to be fully compliant. As one interview participant noted:

> [*Businesses*] *are never fully compliant. I don't think you can be, that's the thing. You're constantly gathering data and so it's like 'are you doing it right every time?' is the question you have to answer. To get the basics in place like your policies and all*

75 Samarin, 8.
76 Samarin, 7.
77 Kwong, 35–40.

that stuff, it just depends on how complicated your data collection practices are, how quickly are you motivated to get this done?" [78]

As an additional challenge, the GDPR and CCPA fail to specify the formats in which user-access requests are to be produced. Research by Yan Fang found that, because of the unclear expectations and non-standard processes used by companies, requesting one's own data can take significant time, as it can be difficult to find the appropriate point of contact and explain your request.[79] There are also difficulties in using or interpreting the data produced because of the incompleteness of the data, or the lack of contextual information provided. Sometimes the data received from user requests are unlabeled, obscured, or otherwise confusing. Some large companies also sent preformulated, non-responsive answers, and some smaller companies failed to respond at all. Consumers can feel uncertain, and even mistrustful, of companies that fail to produce data that they know the companies have.

Costliness

The cost of compliance is a burden that is particularly felt by smaller companies. As mentioned, the GDPR's extensive authority to penalize and fine individuals and small businesses for minor infractions based on vague regulations imposes an unduly high cost.[80] Kwong's research adds that SMEs face time and resource constraints that limit their ability to fully comply, and compliance can take longer than anticipated when attempting to map the data generated and collected by the company.[81]

Serbian startups found that GDPR compliance was worth the cost as it gave them the ability to enter the EU market, but the same was not always true for CCPA compliance.[82] The startups described CCPA compliance as a necessary part of scaling their business, and many conducted CCPA compliance as a precautionary measure since their global customers could be situated anywhere. They noted that, while the CCPA regulation is less demanding than the GDPR, CCPA compliance is more costly because of the need to have a US-based lawyer in order to ensure compliance with other American laws. One such startup needed to partner with a larger company in order to meet these expensive compliance requirements.

78 Kwong, 41.
79 Fang, Yan. "Data Access as Evidence Access." 2021 CLTC Symposium, 11–14.
80 Fan, 42.
81 Kwong, 41.
82 Anđelković, 23.

Non-profits or individuals who create websites are also constrained by the costliness of compliance. In particular, research by Elliot et al. indicated that charities and independent artists needed to re-use and adapt cookie banners they found elsewhere online. Those restrained by limited budgets were very nervous about compliance, and rarely understood the policies.[83] As mentioned, outsourcing compliance through open-source code or plug-in solutions is often cost-prohibitive or requires technical skills.[84] Thus, smaller companies and individuals who are subject to the GDPR may face increased risk of non-compliance because of their constrained resources.

Risk of abuse

As discussed, the ambiguity of privacy laws and lack of oversight over consent interfaces can lead companies to create deceptive designs that deceive users into opting into the use of their data.[85] This is furthered by research indicating that engineers often are made to create consent interfaces that are unnecessarily complicated with legal jargon, making the process of opting out too time consuming for users.[86] Platforms can also impose their own regulations on developers, who lack resources, expertise, and time to effectively comply, resulting in "privacy-unfriendly defaults" and deceptive designs.

Furthermore, both the GDPR and CCPA contain provisions to allow consumers to request their own data from companies, but inadequate authentication of data-access requests could compromise user privacy.[87] Authentication mechanisms that attempt to correct this issue could end up reducing privacy as well, by requiring users to submit too much personal information to verify their identities. Empirical evidence points toward security concerns with authenticating GDPR and CCPA Subject Access Requests (SARs).[88] Teixeira et al. conducted a study by sending out information request emails to websites to ask whether they would process a SAR. Preliminary results indicate that, of the 30 websites initially asked, nearly all responded by email, instead of a phone call verifying that the person requesting was not a bot. The websites all had variable methods of verifying identification: some required sending an email from the relevant email address, while others had a vague "identity must be clear"

83 Elliot, 12.
84 Elliot, 14.
85 Kyi, 1.
86 Grover, 3.
87 Fang, 15–16.
88 Teixeira, Ross, Gunes Acar, and Jonathan Mayer, "The Right to Data Access: A Million-Website Comparative Analysis of GDPR and CCPA Implementations." 2021 CLTC Symposium, 1.

standard. Many were vague about what information is provided in response to the SAR.[89] The final results of the study are yet to be determined, but the researchers' preliminary findings indicate that companies have not yet ascertained a secure and safe method of providing information pursuant to SARs.

Issues with enforcement

Research on enforcement, limited to the GDPR because the CCPA has not yet fully rolled yet, reveals how a lack of resources and expertise can limit effective GDPR regulatory action and how the GDPR's broad scope can produce disparately harsh enforcement on individuals and small companies.

Lack of resources and expertise

Regulators face complications with enforcement mechanisms and resources that get in the way of effective enforcement. Sivan-Sevilla's research, based on a questionnaire filled out by seven DPAs, interviews with DPA employees, and secondary sources, indicates a national divergence in enforcement style.[90] In contrast to the research by Li et. al. explaining the increased potential for cross-border accountability and consistent enforcement, Sivan-Sevilla argues that lacking organizational capacity, such as experts and budgets, and budgetary autonomy can negatively impact DPA behavior and show the top-down failures of the GDPR.[91]

Sivan-Sevilla's research shows that lacking adequate budget and expertise limits the organizational capacity of the DPAs, which leads to differentiating enforcement styles. DPAs with wide monitoring strategies but insufficient resources and low organizational capacities — such as in Belgium, The Netherlands, Romania, Czech-Republic, and Slovakia — had a low tendency to fine and investigate violations.[92] These DPAs struggled to translate their supervision strategies into adequate enforcement action because of they lacked organizational capacity, reflecting the importance of adequate budgets and expertise.[93] DPAs with external motives, such as budgets that were reliant on fines, were more likely to investigate and place fines, even when they lacked resources. When there was no external motive to impose fines, DPAs chose to use fines only in the minority of their enforcement decisions, despite the ability to strictly enforce

89 Teixeira, 6–9.
90 Sivan-Sevilla, 1.
91 Li, 26-28; Sivan-Sevilla, 1.
92 Sivan-Sevilla, 21.
93 Sivan-Sevilla, 20.

such penalties.[94] The discrepancy in their reluctance to fine demonstrates how GDPR enforcement could be selective and inconsistent among DPAs.[95] While Li et al. make the argument that One-Stop-Shops like those in Ireland and Luxembourg are effectively held accountable by peer member states, the question still remains whether other nations with fewer resources and external motives have as much incentive, or ability, to investigate and penalize GDPR violators.[96]

Disparate effect on individuals and smaller entities

Enforcing vague regulations like the GDPR imposes unfair and disparate effects on smaller companies and individuals.[97] In line with their intentions, privacy regulations should target entities with data-intensive practices that have the ability to exact serious harm and have the resources to understand potential violations. Furthermore, individuals and smaller businesses are less likely to have the resources to comply with the GDPR and defend themselves when accused of violations. As mentioned, the vagueness of Article 5 disproportionately punishes individuals and small companies, and the result can be damaging: violations of Article 5 can result in a penalty of 20 million euros [approximately US $23.5 million] or four percent of revenues of the prior year, whichever is higher. An inability to pay such fines can result in substitute incarceration. In addition to administrative penalties, GDPR complainants can seek judicial remedies for infringements.

The ability to impose large fines, and even incarcerate individuals, based upon unclear and malleable GDPR provisions can result in the abuse of enforcement powers. As seen with the Turkish kebab restaurant owner and employee, failing to safeguard individuals and small businesses can produce disparate enforcement of the GDPR on marginalized communities.

EXTERNAL EFFECTS AND INNOVATION

While most research presented at the symposia analyzed the effect of the laws on compliance, researchers have also noted where the GDPR and CCPA affect business practices and product development. In analyzing SEC filings, Wong et al. noted that large technology companies perceive that privacy legislation and risks limit the development of new, data-intensive prod-

94 Sivan-Sevilla, 18.
95 Sivan-Sevilla, 6.
96 Li, 21–22; Sivan-Sevilla, 20–22.
97 Fan, 22.

ucts. [98] Their research also indicates that the GDPR and CCPA have decreased large companies' advertising revenue, marketing capabilities, and ability to work with enterprise clients. Companies like Facebook and Airbnb have voiced their concerns with how the laws would limit their advertising revenue and marketing. Salesforce noted that they would need to spend resources to vet enterprise clients and evaluate their compliance.[99] This could be a heavy cost for companies, and a big win for regulators wanting to limit the collection and processing of user data. But as mentioned, this evidence only indicates how companies are signaling their intentions to investors — *not* whether they have *actually* limited these products and practices.

Smaller companies could be forced out by the high costs and resources required to be compliant with the GDPR and CCPA. Startups in Serbia found the GDPR had a high impact on business development, which can be explained by the law's broad scope and applicability to all companies, regardless of size or intensity of data practices. The GDPR restricts the transfer of personal data to other countries or international organizations, and requires that all data collection must be stored in the EU or within similarly protective jurisdictions.[100] Startups noted that this was a challenge for those operating in countries beyond the EU. The higher impact of the GDPR on business could have raised barriers to entry for startups by slowing down their marketability.[101] Startups that are compliant with the GDPR specifically noted that their marketing was limited by Article 21, which allows consumers to request that their personal data not be used for marketing purposes. But these startups emphasized that the cost of adhering to the GDPR was offset by the benefits of entering the EU market. Compared to complying with patchwork data regulations from each EU member state, GDPR compliance gave them a one-ticket entry into the entire EU market. This indicates how transnational regulations incentivize startups to emerge and build compliance frameworks from the ground up, even when the cost of compliance is high.

Although the CCPA had a lower impact on the startups' business development than the GDPR, the nature of the CCPA also imposes high barriers to entry. The CCPA differs from the GDPR in that it is a sectoral law regarding consumer rights. This meant that Serbian startups, such as one specializing in workforce quality assessment, have to ensure additional compliance with other US laws, like the Equality Act. Because of the prohibitively higher costs, the startup had to partner with a bigger company to remain compliant. This indicates that the CCPA could limit the ability of startups abroad that specialize in such industries to operate independently.

98 Wong, 12.
99 Wong, 13.
100 Anđelković, 15–16.
101 Anđelković, 22–23.

It is important to note that this research was limited to Serbian startups, and more research is needed to analyze whether startups in other nations have been forced out by the prohibitive costs of the GDPR and CCPA.[102]

LIMITATIONS ON THESE STUDIES

It is important to note that there is less coverage of the CCPA compared to the GDPR in these studies. This is explained both by the limited scope of the CCPA in terms of geographic area and number of affected people and entities, and its shorter period of enforcement. While the research on the GDPR may predict the effect of the CCPA and other privacy laws (see below), more time is needed after the CCPA is fully rolled out and augmented by the CPRA to research and analyze its effect on stakeholders. More time may also be required to determine the effect of both laws on innovation.

102 Anđelković, 22–23.

II. Lessons learned & recommendations

Research Question: "How do the experiences of stakeholders inform how to better comply and enforce the GDPR and CCPA/CPRA, and meaningfully improve privacy protection?"

The research papers presented at the CLTC symposia shed light on how companies can better comply with — and how regulators can better enforce — the GDPR and CCPA to more meaningfully improve privacy protections. Below are recommendations for companies that are subject to these regulations, as well as the regulators that enforce them.

RECOMMENDATIONS FOR COMPANIES

Stakeholders subject to the regulations of the GDPR and CCPA/CPRA can adjust their operations to better and more efficiently comply by framing compliance as business risks, adjusting organizational practices, preventing deceptive designs, and securing their compliance processes.

Frame compliance as risk prevention

Companies can more effectively motivate GDPR and CCPA compliance by reframing compliance as risk prevention, rather than just focusing on abstract user-centric privacy concerns. As research by Wong et al. showed, companies are motivated to point out, predict, and prepare for privacy issues in their SEC filings because of the regulatory risks, reputational risks, risks to internal business practices, risks to external stakeholders, and cybersecurity risks.[103] Investment is a site of debate over privacy values, as shown by the success of shareholder activism in shaping how companies disclose climate change risks and in shifting Apple's and Microsoft's practices regarding the right to repair.[104] Research by Anđelković et al. regarding Serbian startups indicates that smaller companies find that the cost of lower investments or withdrawn investments are more effective than fines in ensuring compliance

103 Wong, 1.
104 Wong, 19.

with these laws.[105] Viewing privacy as a business risk can also help privacy practitioners within companies advocate for privacy reform in ways that are actionable.[106] A user-centric ethos to privacy protections may not convince a company to change its course, but reframing privacy protections as business and investment risk mitigation could be more effective.[107]

Encourage organizational cohesion and prevent deceptive designs

There are undeniable frictions between the priorities of lawyers responsible for ensuring compliance and the interests of front-end implementers (designers and developers) responsible for developing user-friendly interfaces. Front-end implementers and legal teams need to work more collaboratively with each other in creating cookie banners that are easy to navigate and understand, rather than simply complying with the letter of the law, to prevent deceptive designs that potentially deceive users to opt in.[108]

Companies can provide better support to employees who create data-consent interfaces by engaging outside experts and creating clear, user-centric requirements for front-end implementers. Companies can look to processes used in the financial services industry, where, despite the complex laws involved, specialized knowledge is not required to integrate payment processing on websites. For these payment systems, legal text is not prioritized in the user interface. Instead, these sites employ user design elements that center end users' needs and understanding, all while remaining in compliance with relevant laws. By integrating user habits and psychology, as well as understandable language, in the interface of cookie banners, companies can prevent deceptive designs from emerging while ensuring they are in compliance.[109]

Where legal and compliance experts are not available, developers are often left responsible for privacy compliance in their companies, which can lead to a lack of oversight, accountability, and potential noncompliance.[110] Firms can overcome this by encouraging more transparent communication and sharing updates about compliance to encourage developers to demonstrate and confirm the impact of their work. To ensure that developers do not regard privacy as just a "check box" in their code review,[111] research by Grover showed that using

105 Anđelković, 23.
106 Wong, 19.
107 Wong, 19.
108 Elliot, 2.
109 Elliot, 15–16.
110 Grover, 14.
111 Grover, 15.

metaphors can help tech workers better understand the ubiquitous importance of privacy protection. For example, drawing a comparison between privacy protection and content moderation — and highlighting that they share the same goal of cultivating community-oriented goals — can help boost quality. Furthermore, reframing privacy concerns as business risks, rather than user-centric issues, can help shift organizational practices more effectively and better encourage compliance.[112]

Ensure sufficient verification of consumer data requests

As Samarin et al. noted, many companies may be failing to adequately verify consumer requests for information, and could be risking the inadvertent sharing of personal information with impersonators.[113] For companies that maintain user accounts, the researchers advise relying on existing authentication mechanisms and, at the very least, requiring a password to submit requests, verify identity, and access the provided data. Ideally, companies should require multi-factor authentication, such as mobile push notifications or one-time passwords. Companies should also notify users about VCR submissions using existing communication channels to help consumers detect fraudulent requests for their data.

Companies that do not require the creation of user accounts should request at least three pieces of user-specific information to match against the data already held by the company. If the company does not receive sufficient information to verify the consumer, then they should reject the request. Companies should *not* request copies of government-issued IDs for authentication, as most organizations would not have access to unique ID numbers to match against, and other information on such IDs, such as name or date of birth, can be easily digitally altered. Once a company has successfully verified the VCR, it should provide secure access to and transmission of consumers' personal information. Companies can use existing authentication mechanisms, multi-factor authentication, TLS encryption, download links with a time expiration, and secure files using a password set by the consumer beforehand.[114]

112 Wong, 19.
113 Samarin, 12.
114 Samarin, 13.

RECOMMENDATIONS FOR REGULATORS

Regulators can more effectively serve the goals of the GDPR and CCPA by creating a safe harbor for individuals and small entities under the GDPR, clarifying ambiguous language, monitoring and taking action on deceptive designs, employing an explicit advisory function, and permitting data sharing for social science purposes.

Create a safe harbor for small business and individuals under the GDPR

Research has shown that vague and large penalties imposed on small businesses and individuals can lead to devastating, and often discriminatory, enforcement of privacy laws.[115] Fan recommends that regulators provide safe harbors for individual persons and small businesses with fewer resources. The EU should take inspiration from the CCPA and other US privacy proposals, which often focus penalties on entities and persons with more power to perpetrate privacy harms, and who have the ability to realistically meet regulatory standards, address problems, and defend themselves in penalty proceedings.[116] The CCPA limits enforcement to entities that (1) had more than $25 million dollars in gross annual revenues in the preceding year; (2) annually buy, sell, or share the personal information of 100,000 or more households; or (3) derive half or more of their revenues from selling personal information.[117] The CCPA also limits the private right of action to data breaches, whereas the GDPR allows complaints to be brought for *any* infringement of the GDPR's numerous and broad obligations. This limitation in the CCPA is heavily contested, and many argue for a broader private right of action, but as mentioned, the GDPR's broad right of action powers can lead to overenforcement toward individuals and small businesses.[118]

Exemptions or safe harbors for those least well-situated to defend against privacy penalty proceedings is an emerging better practice that has important lessons for the EU's GDPR and its international emulators. Such exemptions could prevent DPAs from imposing harmful financial and criminal sanctions on marginalized communities for violating the GDPR.

115 Fan, 4-5.
116 Fan, 44.
117 Fan, 21–22.
118 Fan, 22.

Clarify ambiguous language with specific definitions and guidance

Fan also suggests that regulators must specify the basis for criminal and civil offenses, particularly for GDPR Article 5.[119] Individuals and small business defendants most often find themselves in violation of Article 5 because regulators have broad, sweeping powers in interpreting and enforcing the vague language of Article 5. Regulators should follow the language used in Article 32, used most often against major corporations, which includes specific examples of infractions. More specific penalty provisions will help prevent privacy harms by providing individuals and organizations with clearer guidance on how to comply, and will also reduce the risk of arbitrary and discriminatory enforcement.[120]

Research on the growth of data breach notification laws suggests that privacy laws should be careful with how they address certain technological innovations, such as encryption.[121] Some states have enacted data breach notification laws that exempted organizations from disclosing breaches that involve encrypted data. But some companies broadly interpreted this exception to justify failing to disclose breaches involving the loss of encrypted data that could have been decrypted. As a result, states tightened the disclosure exception to exclude encrypted data that was stolen along with the encryption key. This change in language led to a decrease in identity theft reports, indicating the importance of clear language around how to handle advanced technology without unintentionally creating exceptions that are broader than necessary.

Furthermore, privacy regulators should be vigilant in ensuring that companies are actually complying with the intent of the law. In his research study, Aniket Kesari correctly predicted that companies would fail to follow the intent of vague provisions, as seen in deceptive designs emerging on many websites' consent interfaces. Regulators should be careful to make sure any other provisions do not unintentionally protect actions that do not align with the intent of these laws.[122]

Monitor and take enforcement action on deceptive designs

Regulators should create more explicit guidelines for how firms can give users effective and informed consent, which will help prevent deceptive designs that mislead users and result in the misuse of data by controllers. Some researchers argue that regulators should use automation to

119 Fan, 43.

120 Fan, 43.

121 Kesari, Aniket. "Do Data Breach Notification Laws Work?" *NYU Information Law Institute* (August 30, 2022). Available at SSRN: https://ssrn.com/abstract=4164674 or http://dx.doi.org/10.2139/ssrn.4164674, 47; Mahoney, 6; Kyi, 45.

122 Kesari, "Do Data Breach Notification Laws Work?," 47; Mahoney, 6; Kyi, 6

ensure compliance with privacy laws in consent interfaces. Furthermore, consent management providers (CMPs) can provide illegal interfaces to a large swath of website clients, meaning their infringement affects providers, advertisers, and users. Because of the popularity of CMP services, regulators should require that CMPs only offer compliant consent notices.[123]

The prominence of deceptive designs in the consent interfaces required under both the GDPR and CCPA has led some researchers to suggest that regulators move away from notice and consent provisions entirely.[124] Users have inadequate information about their rights and do not understand their ability to exercise them, which prevalent deceptive designs take advantage of. Even when deceptive designs are not present, cookie consent banners present an information asymmetry; users will never be able to know enough about where their data is going or how it will be used. Therefore, regulators should find more understandable and less deceitful ways of collecting consent with fewer steps for users.[125]

Mahoney suggests that regulators should impose a blanket prohibition on processing data that is not required to provide the service requested by the consumer, limiting companies' data collection to narrow operational use. This would require strong enforcement to ensure compliance, but it would be more effective than the opt-in and opt-out interfaces.[126]

Add an explicit advisory function to monitoring and enforcement mechanisms

Regulators should take on more of an advisory, rather than just a quasi-prosecutorial, role in helping stakeholders prevent violations and creating effective and fair enforcement.[127] Both the CCPA and the GDPR have independent agencies tasked with enforcement: the CPRA established the five-member California Privacy Protection Agency (CPPA), and the GDPR deploys DPAs in each member state as independent public authorities. While an independent agency with strong enforcement power may be part of the approach, Fan argues that an overfocus on the prosecutorial function can create issues by focusing more on punishment than harm prevention. A more explicit advisory function, on the other hand, could expand the agency's function to focus more on harm prevention. While the CPRA outlines the advisory role of CPPA members, Fan emphasizes the importance of separating the roles of regulators who offer guidance from the investigative, prosecutorial, or advocacy roles.

123 Mahoney, 6; Kyi, 6.
124 Kyi, 9–11.
125 Kyi, 14.
126 Mahoney, 1.
127 Fan, 46.

Permit and encourage data sharing with verified social science researchers

Companies must comply with privacy laws and secure user data, but some situations require sharing data with researchers in order to remedy or help prevent catastrophic data privacy infringements (i.e., the Cambridge Analytica scandal, where the consulting firm used the personal data of millions of Facebook users without their consent for political advertising). Newly enacted laws in the EU — the Data Governance Act (DGA) and the Digital Services Act (DSA) — may compel large platforms to make certain data available to researchers.[128] But these laws may unintentionally limit the scope of accessing the data and the types of data available for researchers.[129] The DGA encourages data sharing through trusted intermediaries, but that is complicated by the GDPR's restrictions on data re-use and cross-border data sharing. All efforts pursued through the DGA must maintain GDPR compliance, yet appropriate strategies to do so remain unclear. The potential risks of violating the GDPR may inadvertently cause the public and private sectors and individuals to refrain from sharing data with the intermediaries. The DSA, on the other hand, can compel platforms to make data available to researchers to assess potential harms or noncompliance, but similar to the DGA, it is unclear how platforms can do so while remaining GDPR-compliant. Nonnecke et al. suggest that regulators clarify how platforms can remain compliant with the GDPR under the DGA and DSA to encourage, rather than deter, data sharing for social science.[130]

Finally, partnerships between platforms and independent researchers need to be strengthened. In the wake of the Cambridge Analytica scandal, Facebook struggled for 20 months to share the relavent dataset with public interest researchers because of the company's uncertainty about how to maintain GDPR compliance. Facebook's market value fell by more than $36 billion as a result of the scandal, not to mention the harm caused to over 87 million Facebook users. Regulators, companies, and other stakeholders have an incentive to give researchers appropriate access to data in these circumstances. But regulators must create clear provisions on how companies can remain compliant with privacy laws when they grant data access to researchers.[131]

128 The DGA, which was put into effect on June 23, 2022, facilitates data-sharing by making public- and private-sector data available for research and commercial purposes, including the reuse of data for "altruistic goods." The DSA, which entered into force in November 2022, requires platforms to make data available to researchers to support transparency, accountability, and legal compliance.

129 Nonnecke, Brandie, Camille Carlton, and Varsha Vaidyanath, "Data Sharing for Social Science Research." 2021 CLTC Symposium, 4–5.

130 Nonnecke, 7–8.

131 Nonnecke, 7–10.

III. Anticipating the effects of emerging laws

Research Question: "How does empirical evidence of the effects of the GDPR and CCPA/CPRA anticipate the effects of emerging privacy legislation?"

The empirical evidence from the papers presented at the CLTC symposia can help us anticipate the effects of emerging privacy laws, and provide suggestions for how future legislation can better ensure privacy protection.

SHOULD EMERGING PRIVACY LAWS MIRROR THE CCPA AND GDPR?

As indicated by the spread of data breach laws across the US, privacy laws are likely to continue diffusing across states. But data breach laws in each state vary in the types of information required in disclosures, and to what regulatory agency (or agencies) the information must be disclosed.[132] The same discrepancies are likely to emerge in state-by-state privacy laws, which can create compliance headaches for companies that have customers located in multiple states.

States borrow information from one another, and often will copy text directly from bills from other states or interest groups. New Hampshire, for instance, introduced legislation that is almost identical to the CCPA. But it is not always the case that states closely follow the model of previous laws. Predicting the diffusion of privacy laws by analogizing how data breach notification laws spread across the country, Kesari et al.'s research indicates that overlaps in state data breach laws decreased over time, and newer laws were more and more removed from the first California state law, which passed in 2003.[133] It is not yet clear whether the same is true for privacy law, but as Figure 2 demonstrates, most state laws do not follow the CCPA as closely as the proposed New Hampshire law does.

132 Kesari, "Do Data Breach Notification Laws Work?, 7–10.

133 Kesari, Aniket and Jae Yeon Kim. "Privacy Law Diffusion Across U.S. State Legislatures." 2021 CLTC Symposium, 24–26.

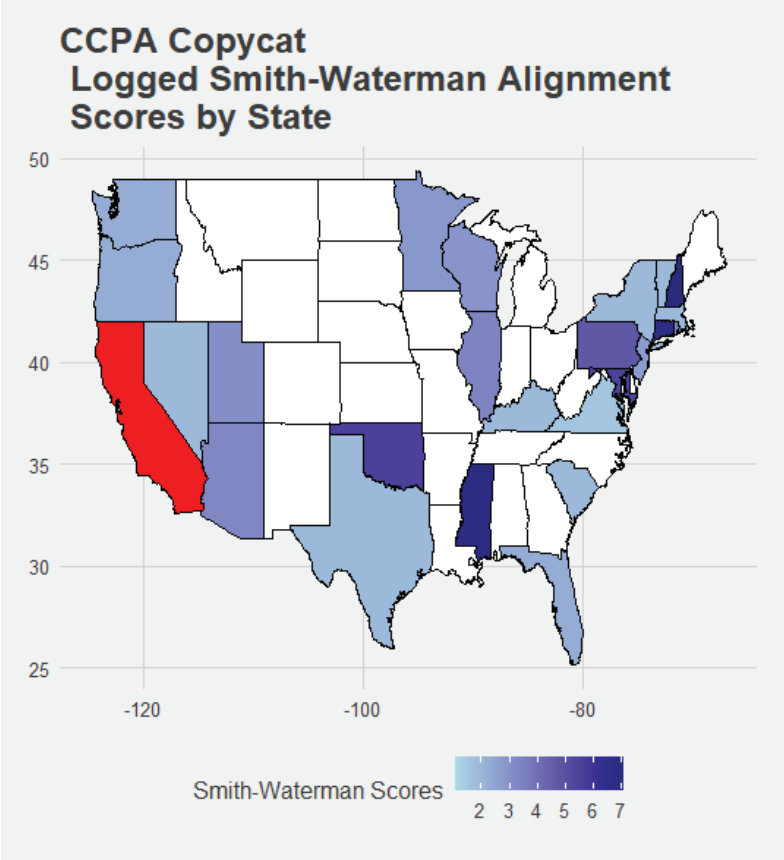


Figure 2. Emerging state privacy laws compared to California in 2021. (Darker color indicates more overlap with the CCPA).[134]

Laws that are more similar to the GDPR and CCPA may find that companies are quicker to comply because they will not have to overhaul existing compliance systems. As indicated from research on how open-source communities responded to the GDPR and CCPA, US state laws that mirror existing laws can reduce compliance hurdles and increase awareness of the new laws in the technical and coding communities.[135] Information derived from an open source repository, Github, suggests that the GDPR and CCPA are perceived as relatively similar in terms of the changes in code required for compliance.[136] This makes it easier for technical communities to update their existing compliance codes in tandem. CCPA awareness and compliance has also likely increased because of its conceptual association with GDPR. The

134 Kesari and Kim, "Privacy Law Diffusion Across U.S. State Legislatures," 20.

135 Nielsen, Aileen. "When Law Makes Code: The Timing and Content of Technical Responses to GDPR and CCPA." 2021 CLTC Symposium, 1.

136 Nielsen, 26.

evidence suggests that Github members more frequently mentioned the CCPA because it was perceived to be substantially similar to the GDPR for purposes of technical discourse.[137]

This research indicates that states can encourage quick compliance by "deliberately crafting statutes that will mirror those already well known rather than in seeking to design state-specific ways of dealing with personal data."[138] By "hooking" into existing laws wherever possible, new laws can minimize legal compliance work for coders and effectively increase awareness of the laws in technical and coding communities. In-house developers, many of whom are largely in charge of compliance frameworks when legal expertise is unavailable, would thus be less likely to fall out of compliance because of these established coding precedents.

Still, widespread mirroring of the CCPA and GDPR does risk further entrenching the less effective, or even harmful, aspects of these policies. Mirroring the language of the GDPR or CCPA could limit the protection of user privacy to the effectiveness of those laws, rather than improving user data protection, and could proliferate their unintended consequences. As mentioned, the vague language of the GDPR and CCPA creates uncertain and unstable compliance measures, while also harming consumers when companies find loopholes — for example, in what counts as a "legitimate interest" in collecting data. Integrating the ambiguous provisions of the GDPR and CCPA into new privacy laws can also create more compliance confusion if each state interprets and enforces each of these provisions differently.

PROCEDURAL LESSONS

The enactment and enforcement of the GDPR and CCPA pose important lessons for emerging privacy legislation. Aileen Nielsen's research indicates that key legislative dates serve as strong communication to and deadline mechanisms for the technical community preparing for compliance processes.[139] In particular, the date when the law becomes enforceable is where the most activity arises from the technical community. The date of the laws' adoption had little to no activity from the technical community. But for the GDPR, where the date of enactment was the date that enforcement began, the date the law entered into force was the primary date of activity. For the CCPA, which had a pre-announced six-month delay in enforcement activity following the law's enactment, most of the issue-filing activity occurred after enforcement action began.

137 Nielsen, 30.
138 Nielsen, 27.
139 Nielsen, 29.

But Nielsen's research further suggests that the time between the CCPA's passage and enforcement was longer than was necessary or even desirable. Presuming it is in the public interest to enforce data protection policies as soon as possible, and without any other compelling interest in a longer preparation period, the evidence suggests that writing code for legal compliance does not require such a long amount of time. That time was largely unused by the open source community to adapt to and prepare for these emerging laws. Therefore, emerging laws need not delay enforcement, especially when the laws are similar to the CCPA and the GDPR, as their compliance codes already largely exist.[140]

SHOULD THERE BE A FEDERAL PRIVACY LAW?

The emergence of privacy laws across several U.S. states has prompted the question of whether a federal privacy law would better serve users' privacy interests and establish more consistent and manageable compliance standards. Kwong suggests that a federal privacy law would especially help small- and medium-sized companies that have already struggled with competing standards across a patchwork of existing legal frameworks.[141] Larger companies have the resources to effectively comply, and they often adopt global compliance strategies even when the law does not require them to do so.[142] But competing standards make it impossible to create strategies for smaller companies without incurring large financial costs, making effective compliance unnecessarily burdensome. This is especially challenging for companies without previous experience with such regulations.[143] Furthermore, a federal law could bring states without data privacy laws up to a minimum standard.[144]

In order for a federal law to smooth over the patchwork of state law requirements, it would require preemption. Preemption would allow for a federal law to effectively supersede existing state privacy laws, such as those in California, Colorado, Connecticut, Utah, and Virginia. It sets a ceiling, rather than a floor, for regulation, meaning that states cannot create stronger privacy protections than a federal law would require.

Supporters of state-by-state privacy laws fear that a federal privacy law that preempts state law would ultimately inhibit privacy protection. Individual states can experiment with different

140 Nielsen, 29–30.
141 Kwong, 17–18.
142 Kesari and Kim, "Privacy Law Diffusion Across U.S. State Legislatures," 4.
143 Kwong, 17–18.
144 Kesari, "Do Data Breach Notification Laws Work?," 42.

regulatory responses and can more quickly respond to new technology developments, resulting in stronger privacy protections than a federal law could provide.[145] Looking at the regulation of fields that involve similarly complex and rapidly advancing technology, such as with data breaches, sheds some light on this issue as well. Amendments to state data breach notification law have driven policy innovation that could better protect consumer data and respond to emerging privacy issues, such as encryption.[146] Kesari notes that while a federal data breach notification law could reduce compliance costs, preemption would prevent state regulatory innovation that would be more reactive to and effective at reducing harms.[147] The ability to quickly change such regulations is especially important when considering the regulatory uncertainties and emerging risks of abuse that resulted from the GDPR and CCPA.

There have been several attempts at passing a federal privacy law, most recently the American Data Privacy and Protection Act (ADPPA) in 2022. With some exceptions, the bill generally preempts existing state law.[148] Representatives from states without existing privacy laws argue that their constituents deserve privacy protections now and cannot wait until their states enact their own privacy laws, if they ever do.[149] But others have voiced concerns that preemption and congressional gridlock could prevent critical modifications to a federal privacy law in the face of rapidly advancing technology.[150]

The debate over federal versus state-by-state privacy regulation remains contentious, and it is unclear if, or when, further action on the ADPPA or any other potential federal privacy bill will occur. But observing the existing effects of the GDPR and CCPA and the evolution of data breach notification law can help predict the risks and benefits of such privacy regulation proposals.

145 Kesari and Kim, "Privacy Law Diffusion Across U.S. State Legislatures," 3.

146 Kesari, "Do Data Breach Notification Laws Work?," 44.

147 Kesari, "Do Data Breach Notification Laws Work?," 43.

148 Duball, Joseph. "State views on proposed ADPPA preemption come into focus," International Association of Privacy Professionals, September 27, 2022. https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/.

149 Duball, "State views on proposed ADPPA preemption come into focus."

150 Duball, "State views on proposed ADPPA preemption come into focus."

Conclusion

The GDPR and CCPA were the first ventures into the world of data privacy protection laws, and although numerous U.S. state laws have emerged in their wake, we are still on a long road to finding solutions to privacy issues. As empirical evidence from the CLTC symposia papers indicate, some provisions of the GDPR and CCPA are working well while others are not. The intent of the GDPR and CCPA can be disconnected from their on-the-ground effects, as seen with the emergence of deceptive consent interface designs. Still, some argue that emerging privacy laws should mirror the GDPR and CCPA to reduce regulatory inconsistencies, despite hurdles firms face in complying with these existing regulations.

This paper has provided suggestions to regulators and firms to help avoid such issues, but the question remains whether an altogether different approach would be more appropriate. Viewing the GDPR and CCPA as "first drafts" of how to regulate data protection and privacy reminds us that these laws, although they were among the first, are not the only methods of protecting data privacy. Future research on how other regulatory frameworks could more effectively protect privacy — rather than how to circumvent or correct the GDPR's and CCPA's misaligned results — could get us closer to the intended goals of data protection and privacy regulation.

Acknowledgments

The author thanks the UC Berkeley's Center for Long-Term Cybersecurity and the 2021 and 2022 CLTC research symposia participants. The author particularly wishes to thank Ann Cleaveland, Chris Hoofnagle, and Jeeyun (Sophia) Baik for their thoughtful feedback and suggestions, and Jordan Famularo for her helpful guidance. The author also wishes to thank Rachel Wesen for her assistance finalizing production and Charles (Chuck) Kapelke for his valuable edits. This research was made possible by the William and Flora Hewlett Foundation, the Charles Koch Foundation, and Meta in support of independent academic research.

About the Author

Saba Chinian is a third-year law student at the University of California, Berkeley, School of Law and a Graduate Student Researcher at the UC Berkeley Center for Long-Term Cybersecurity. She can be reached at saba.chinian@berkeley.edu.


CLTC
Center for Long-Term
Cybersecurity
UC Berkeley