An Analysis of Privacy-Impacting Regulatory Efforts and Their Effects on Service Providers and Individuals

Andoni Gorostiza
andonig@knights.ucf.edu
University of Central Florida
Orlando, Florida, USA

Jordan McMillan
jmcmillan@knights.ucf.edu
University of Central Florida
Orlando, Florida, USA

ABSTRACT

Various governing bodies from around the world have attempted, with varying levels of success, to impose regulatory efforts on the usage of the internet by its citizens, with reasons for said efforts often based in censorship, politics, and privacy. In this comprehensive analysis report, we look into various attempts of regulatory efforts, observe any changes that resulted from imposing said efforts, and attempt to contrast results to a general expectation of privacy. Multiple attempts throughout history will be assessed, and upon doing so, we will understand their outcomes, underline the literacy of the regulations, look for potential circumventions of said regulations, assess their impact to privacy, and predict future trends.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; *Social aspects of security and privacy*.

KEYWORDS

legislation, privacy, service providers

ACM Reference Format:
Andoni Gorostiza and Jordan McMillan. 2022. An Analysis of Privacy-Impacting Regulatory Efforts and Their Effects on Service Providers and Individuals. In *Proceedings of (CAP 5150)*. ACM, New York, NY, USA, 7 pages. https://doi.org/XXXXXXX.XXXXXXX

1 INTRODUCTION

Privacy is a topic that often flares up in human consciousness. While modern advances in technology have yielded significant improvements in quality of life across the world, it has come with drawbacks as well. Privacy has been a human concern throughout history, and this concern has only been amplified by computers, cameras, and other advances. The ability to maintain one's own privacy rapidly evaporated with these inventions. As such, external entities must shoulder this responsibility.

Governments have been seen to step in to be the primary entity responsible for ensuring privacy. They pass legislation and create other forms of regulation that impact the privacy of their citizens. Depending on the motivation of the legislating body, these regulations are able to improve or remove privacy. Most, however, are benign.

It is the goal of this paper to analyze such regulations to determine their actual and intended impacts, their target entities, and the potential future of related regulations. In doing so, it is possible to advise on future regulation to improve human privacy. The final contribution is a generalizable approach to analyzing privacy regulation, as well as specific analyses and trends in legislation noted by the authors.

2 METHODOLOGY

Regulations, whether through legislation or some other governing body effort, are sampled from online databases [15] with keywords pertaining to *Internet*, *Data Privacy*, *Data Protection*, *Net Neutrality*, and *Privacy*. Origins were taken into account to prevent an oversaturation of regulation from isolated geographic regions or nations. Separate from the sampling is the General Data Protection Regulation (GDPR), which marks in our consideration the beginning of modern regulatory efforts.

In order to understand the outcomes of particular regulation attempts, each selected regulation is examined to see what entities are affected. Using GDPR as a baseline, the impact is measured in terms of impact on the entity (processing overhead, adoption difficulty, etc.), the adoption rate of the regulation guidelines (whether the entities actually comply), and the effect on user privacy if applicable. Impact is respectively determined historically through publications by service providers and research examining coverage.

Literacy of the regulations will be examined through the lens of definitions used in the regulation. For instance, GDPR considers data holders to be anyone that collects and stores data from European Union (EU) citizens. Understanding this helps to understand why a regulation is or is not impactful, and helps in predicting future trends. Additionally, the definitions and overall technical literacy of a regulation leads directly to potential circumventions. If any existing circumventions are found that do not rely on lack of enforcement, the literacy must be examined to discover why. After such examination, each legislation will be judged in regards to the following characteristics:

- Compliance Impact,
- Technical Literacy,
- Jurisdiction and Reach,
- and Monetary Impact.

Future trends in regulation will be predicted by summarizing the previous metrics, and temporally analyzing how literacy changes over time. These predictions rely on an assumed enforceability of regulations enacted.

CAP 5150, 2022, Orlando, FL

ACM ISBN XXXXXXX.XXXXXXX…$0.00
https://doi.org/XXXXXXX.XXXXXXX

3 GDPR

The privacy landscape changed significantly with the enactment of the GDPR in the EU. It went into effect in May of 2018, and changes in response are still seen today. As such, current events in privacy are considered in a post-GDPR lens. In this section, we analyze the impact GDPR has had on service providers, as well as the impact seen on and in other governing bodies. For an example of each: GDPR has led to the advent of cookie consent forms [18] and many African nations have been seen enacting similar policies.

3.1 Service Providers Under GDPR

Service providers who store information about their users make up just about all service providers who use the internet as a platform. As such, under GDPR, any website seen would be required to alter their practices for residents of the EU. Most of these are behind the scene changes in how these providers obtain, process, and potentially share data. However, some changes are visible to users and require some user input. We go over both of these categories, analyzing the efficacy of the measures, whether or not they are typically adopted, and determine their impact on the service providers.

3.1.1 Behind the Scenes Data Processing. GDPR outlines rules of how EU residents' data must be held and processed with the intention of strengthening their privacy rights in the digital age. This ends up applying to the data of any user, as it is impractical for a service provider to separate their data from others'. One reason for this is the impossibility of perfectly classifying a user as being an EU resident or not. Any false negative (EU resident misclassified as non-EU) would violate the GDPR, and as such it is safer to assume that any user is in the EU.

As a service provider processing data, GDPR directs that one has to consider that not all data is equivalent in terms of privacy impact [21]. Any data processor must have some classification of their collected data and with that classification some guidelines on how different classes data may be used. This seeks to ensure providers are aware of the data that they hold, which allows any enforcing body to hold them accountable. In this regard, it is an effective measure. However, due to the opaqueness of this process it is impossible to gauge its adoption rate. The only time this measure would come up is if some processor were to commit some violation and receive an audit.

Additionally, according to Article 32 of the GDPR data holders should at all times seek to encrypt and anonymize data they possess, if possible. While the impacts of this are not seen by the users, they are visible in the event of any data breach. This was considered good practice before the GDPR, so the adoption rate for reputable service providers is high. The technology for these measures is mature, so they are easy to implement for providers and yield little overhead for processing and service provision.

3.1.2 User-facing Changes. When visiting popular websites, it is common to see cookie consent forms. The most common form is an acknowledgement that the website (service provider) uses cookies, and provides a link to the provider's privacy policy [14]. Oftentimes, these are obtrusive to the user and the only way to dismiss them is to give the provider one's acknowledgement, and hence their consent to the use of cookies. In this way, these consent dialogues provide only for an appearance of GDPR compliance. They do little to provide for any additional user privacy and require nearly no effort for provider implementation.

A variant of the cookie acknowledgement form is a robust cookie consent form that allows a user to specify which cookies or classes of cookies are and are not okay for use and storage. This system provides for much potential for user privacy, but suffers two primary problems [14]. 1) For the user, this is relatively involved and a non-technical user cannot make an informed decision and 2) for the provider this system is difficult to implement and for some services is nonviable.

Reaching a middle ground of these approaches would be ideal to maximize the potential for user privacy while minimizing the difficulty and problems a provider might experience in the implementation. However, any variant suffers the issue of an uninformed user making an informed decision. Abstractions of cookie purposes have to be made so that the average user can properly provide informed consent, but these are woefully lacking. Perhaps a solution would be the reduction in cookie amount so only vital cookies to services rendered are present, which are easier to explain than tracking cookies.

GDPR also requires a provider to allow users to request the data held on them, as well as complete deletion of that data [21]. This is one of the most strongly enforced features of GDPR with respect to data deletion. For a technically literate person, the data they may retrieve allows them to make future informed decisions. For the average user, this allows for removal of their data simply by citing the GDPR rather than having to jump through whatever hoops the provider may put them through. The removal of this data, such as upon account deletion, gives the user the assurance that if in the future the provider is to suffer a data breach (as is likely to occur at some point in time), their data would not be a part of it. This can be particularly challenging for the provider to support, especially with respect to the request to download existing data. As such, most providers support these for compliance with GDPR, but do not advertise these services or provide forms for them [13].

4 MODERN REGULATIONS

In the wake of the EU's GDPR, there has been an incredible amount of legislation throughout the world related to privacy. Specifically referring to data, there have been hundreds of pieces of legislation proposed and enacted [15]. Perhaps the most well-known in the United States would be the California Consumer Privacy Act (CCPA), which was enacted in 2018 as well. Less known, however, is Zimbabwe's Data Protection Act (DPA). These are two pieces of legislation exemplary as being clearly derived from GDPR, but implemented differently. Other legislation will be examined as well in reference to the GDPR.

4.1 CCPA

The CCPA is a more user-empowering version of the GDPR that only applies to California residents. Like the GDPR, residents outside California can often take advantage of the requirements for compliance outlined in the CCPA, however. The key differences

between the CCPA and GDPR are 1) the CCPA has no data processing guidelines 2) private information is more encompassing in the CCPA and 3) data processors are only legally considered as such if they meet certain requirements [3, 21].

The impacts of the CCPA can be seen whenever there is a means of requesting to a service provider that one's personal information is not sold. To this end, it is relatively successful, as any large data processor is obligated to include this option. The rest of the impacts are more opaque, though. A user realistically does not know whether their request for privacy will be fulfilled. In this way, the CCPA is similar to the GDPR. Additionally, no data processing guidelines weakens user privacy, as it does not protect against processor negligence that may weaken privacy.

4.2 DPA

The DPA was enacted in 2021, and thus had time to learn from the prior legislation. It comes with far more power for enforcement, as it only applies to data handlers within Zimbabwe, or handlers that process information in Zimbabwe [16]. In this way, it is quite different from the GDPR. A processor in Germany can do whatever they want with data from Zimbabweans. However, this legislation focuses on enforceability, which is especially important in less politically and economically powerful nations. Compared to the entirety of the EU, Zimbabwe holds little sway and would struggle trying to enforce elsewhere. Besides this, for general purposes the DPA can be considered the GDPR of Zimbabwe.

It is of interesting note, however, that the DPA frequently references the concept of "critical data" as the basis of several other definitions. There is no provided formal definition of such "critical data." This has interesting ramifications for the efficacy of this legislation, which will be gone over in Section 5. Similar to the GDPR, this legislation calls for the existence of some Data Protection Agency. Unlike the GDPR, this legislation specifically forms such a body on a national basis and the positions necessary to support it. The difference in scale is what enables this, and if the GDPR were to first appear as a single country's legislation, then it would be likely that a similar trend would be seen as followed in the DPA.

4.3 PIPL

An interesting GDPR-esque legislation to see is China's Personal Information Protection Law (PIPL). China is frequently criticized for its actions regarding citizen privacy and ability to access service providers (e.g., China's "Great Firewall"). These prior criticisms fly in the face of PIPL, so this legislation presents an interesting case to compare to GDPR in order to see if they still hold.

The legislation holds many similarities to the GDPR. For instance, Chinese citizens, no matter where they may be, should be allowed to request removal of their data, copies of their collected data, and other similar actions. It also uses remarkably similar definitions of a data controller, instead using the term "personal information handler." The uses allowed by a processor, however, are much more stringent. While in the GDPR a processor can use the data if it is in their interest of providing a service, PIPL states that the use of data can only be allowed strictly if one of seven cases are met. The easiest and broadest to meet criterion is handling personal information already disclosed by a person themselves. A possible circumvention of this that still allows processing is making certain details collected on a user during their registration for a service public, thus making that personal information disclosed (despite the unethical nature of such an action) [12]. Additionally, holding a great deal of data on Chinese citizens outside of China is prohibited by PIPL. By enforcing this, the data processor is able to be held to more regulations outside of PIPL.

There are certain penalties associated with breaking the rules of these regulations. For PIPL, they have seemingly copied the GDPR's choice of fining based on a percentage of annual turnover. Interestingly, the fine is potentially higher, as while the GDPR uses 4%, PIPL uses 5%. However, due to the recency of the law and ambiguities in the wording of the fine, it is hard to discern whether the turnover is based on worldwide figures, or is restricted to just China's. Despite being a singular nation's legislation, this is very similar to the supranational legislation of the GDPR, and as such enforcement will be a topic of intrigue due to primarily being concerned with a singular legislating body.

GDPR	CCPA	DPA	PIPL
Billions of USD in fines	Opt-out of data saleability	Arresting political dissenters	Billions of USD in fines
Template for modern laws	Hundreds of compliance changes	Creation of enforcement body	Among first GDPR-esque law in Asia
Advent of cookie consent modals	Auditing privacy policies		
Auditing privacy policies			

Table 1: Modern Regulations Impacts

5 EVALUATION

In consideration strictly of the modern privacy landscape, it is interesting to see how GDPR was essentially the prototype for any comprehensive regulation effort. This gives regulators the option to either strengthen or weaken the guidelines of GDPR for their own use. For instance, in the CCPA it was seen that legislators chose a seemingly weaker set of definitions than chosen in GDPR. The definition of a business as a data holder and processor does not allow the CCPA to hold potentially malicious entities accountable, as these entities can easily allow themselves to fall short of the requirements (e.g., profit) specified in the CCPA. To this end, it is clear that the CCPA is weaker for protecting privacy than the GDPR, which has no such requirements when defining data holders.

Similarly interesting is how different the impacts of these regulations are despite their similar verbiage. This gives the general approach of analyzing literacy through definitions credibility as a viable approach. Outcomes of this approach can be seen in Table 2.

Term	Impact
Annual Turnover	Creation of fines that can impact surpanational corporations
Minor	Requirements for minor data to be held and gathered differently; availability of services for minors
Data Processor	Who the legislation applies to; this definition can shrink or grow
Cookie Consent	Compliance standard of requiring user-consent for tracking cookies
Data Selling Consent	Compliance standard of telling users their data will be sold, and letting them opt-out
Critical Data	Data that can be considered vital to operations for a provider, determines what they can collect and store

Table 2: Key Legislative Terms

This approach also saves human effort and is less susceptible to misreading of legislation as it allows focusing on particular parts of legal documents rather than requiring a holistic understanding, which cannot be expected of one who is not a domain expert.

One particular challenge in the determination of future trends is the difficulty of finding and being able to comprehend regulations written in smaller nations or nations who do not release English translations of their legislation. In light of this, regulation chosen in this paper may be biased toward states whose official language is English. Attempts to find other language regulations were exercised, however even upon finding such regulation it is very difficult to look to the definitions given, as automatic translation tools are not reliable enough, especially when technical language may be involved [23]. Due to this challenge and the consequences of incorrect analysis, legislation that was not able to be found in an officially translated version is not considered.

The outcomes of examining technical literacy of regulations is transferable to legislation outside of the realm of privacy. If legislators are able to better understand the systems they are interacting with and better put into words the effects they wish to bring, it is likely that the digital landscape worldwide would improve. A primary example of this can be seen when Facebook came before Congress in 2018 [1]. There was a clear gap in understanding of terminology related to digital privacy between Facebook representatives and the members of Congress present. Any effort that can close this gap, such as through informed advisement, would lead to more direct regulation. An additional benefit of this would be a reduction in unintended consequences of regulations.

5.1 Impacts and Analysis of Recent Legislation

5.1.1 GDPR. As the most territorially-encompassing legislation seen, GDPR has had very tangible impacts. Service providers have steadily been increasing amounts of privacy preserving features in order to meet compliance standards. For instance, websites that do not feature a sign-up or account feature have been seen to utilize cookie consent dialogs [14] as a way of informing users directly of their privacy policies. This gives individuals who go to service providers a more transparent understanding of how their data may be used, or what data is collected. Small adjustments like this across the Internet have been seen due to GDPR. We see an overall picture of the GDPR, as well as all regulations seen in Table 3. They are given numerical ranks from 1 to 5 based on the evaluation and discussion seen.

In regards to impact on service providers, the implementation of compliance features is left to the providers. Depending on the nature of the data being processed, meeting these standards can be difficult, but even social media giants have found ways to be outwardly GDPR compliant. There have been over 1,000 fines and penalties issued in the name of GDPR [7]. Several notable examples are listed below.

(1) Amazon: In 2021 fined €746 million due to non-compliance with processing principles in Luxembourg [19]
(2) Meta: In 2022 fined €405 million due to non-compliance with 6 GDPR articles in Ireland [8]
(3) Google: In 2021 and 2019 fined in total €140 million in France due to lacking a sufficient justification for data processing activities [4, 5]

Due to these incredibly steep fines that are intended to be noticable even to these incredibly large supranational companies, they have been seen to adopt further GDPR compliance standards. However, as can be seen in the fact that Google was fined multiple times in the same country, it is unlikely that they are all following GDPR to the letter. Regardless, lack of compliance has a definitive negative impact on the companies, such that user privacy stands to benefit.

5.1.2 CCPA. Despite covering a much smaller amount of people, CCPA has been enforced more heavily then past privcy-preserving legislation. It does not come close to the GDPR in terms of fines issued, but has been seen to yield impacts on service providers, like the GDPR. For instance, online retailers are often the recipient of CCPA enforcement action, and after enforcement the regulations are seen to be followed by the service provider. It is not uncommon to see CCPA compliance now, such as when opting out of data forfeiture crops up on many websites. Examples of CCPA enforcement actions can be seen below [17].

(1) Many websites were unclear on what data was used for and did not state if they sold it. After enforcement they included this information in their Privacy Policy.
(2) Sephora was selling user information, did not tell consumers, and did not respond to requests for rectification. They were fined $1.2 million.
(3) Mobile apps have been found to collect and sell data on minors. After enforcement, they were made to separate data based on user minor status and be clear about their practices in their privacy policy.

Law	Compliance	Literacy	Jurisdiction	Monetary
GDPR	5	4	Global	> $1B USD
CCPA	4	3	Regional	> $100M USD
DPA	1	3	Regional	Unknown
PIPL	4	4	Global	> $1B USD

Table 3: Regulations Compared

Thus far, the Sephora case is the only one in which significant penalties have been levied. This shows the CCPA to be much more lenient than the GDPR, as it gives providers notice and time to fix their noncompliance. Whereas with the GDPR, such time has passed that compliance is expected and punitive action can and often does come much more rapidly. Regardless of this lenience, tangible impacts can be seen from the CCPA in favor of protecting user privacy and limiting service providers.

5.1.3 DPA. Due to being very new legislation in the least economically-powerful country whose legislation was considered, DPA enforcement is incredibly limited when compared to either CCPA or GDPR. Interestingly, enforcement action taken in the name of the DPA tends to be individually-focused rather than collectively. For instance, it is possible to find enforcement actions against individuals in Zimbabwe, but not against service providers [22, 24]. What might have appeared to be a data protection legislation to enhance privacy has in actuality been used to stifle freedom.

Individuals that have spoken out against the current governing body of Zimbabwe have been arrested with the DPA cited. This includes a teenager and journalists. This is in stark contrast to anything seen with the CCPA and GDPR, and shows how the impacts of these laws lies solely in how they are actually enforced. Despite being nearly a copy of the GDPR, the DPA has not been used in any way relatable to them. Similarly, it has had no tangible impact on service providers residing in Zimbabwe.

5.1.4 PIPL. As the youngest legislation examined, not much impact has come from China's PIPL. Providers who have received censure at the hands of GDPR in the past may be seen to ensure their compliance with PIPL. Besides this, one notable case of PIPL enforcement can be seen. Didi, a rideshare company that services China, was found in violation of PIPL [10]. The methods and terminology used in the enforcement closely resemble that of GDPR [4], showing how similar these legislations are. Also similar to GDPR was the extraordinarily high fine compared to what is usually seen. Didi was fined over $1 billion USD, which is much more than any single GDPR enforcement action ever yielded.

6 DISCUSSION

While the future is uncertain, there are pre-existing trends that are likely to continue into the future with high confidence. As such, it is possible to make assertions as to what the future may hold when it comes to privacy regulation. The first assertion is that GDPR will expand to essentially become global legislation. The second is that the definition of a data processor will adjust, and the impact of legislation will adjust accordingly. Lastly, privacy regulation is a double-edged blade: just as it can be used to further individual privacy, it can be used to do the opposite.

6.1 Global GDPR

It has been seen that legislation around the world has adopted legislation with verbiage similar to that of GDPR. Between the CCPA, DPA, PIPL, and GDPR this paper has seen GDPR-esque legislation on four continents. Given the occurrence of this over such a short period of time (4 years), it is safe to assume this trend will continue into the near-future. It is not all too unlikely a majority of countries on Earth will have legislation that contains a subset of the regulations outlined in GDPR. In this way, it becomes the Global Data Protection Regulation. Besides this expansion, the extraterritoriality of the GDPR will likely expand into other legislation as well. For instance, it is seen in the PIPL as well, and is part of what gives these pieces of legislation the ability to actually elicit an impact. Even if the legislation did not form in a country, providers in that country would still have to follow the regulations of all the countries with GDPR-esque legislation.

Consequentially, following all the regulations present will become very difficult for service providers. There may become cases that it is not possible to respect one piece of legislation without infringing upon another. In this case, the provider would practically not be able to guarantee adherence to standards. There is no perfectly reliable method of determining one's nationality without collecting information on that user. The collection of such information in the first place may violate some regulation in the future. As such, the expansion of data privacy legislation poses a very difficult situation for service providers moving into the future, and they may be incentivized to lobby against such legislation where they can.

6.2 Data Processor Meaning

A common term between all privacy legislation seen is some form of data processor, or a term with similar meaning. The outlining of what counts as a data processor is vital to determining what service providers must follow the regulations and when they must follow them. However, as legislation can be amended and new laws formed, the definition of data processor can change. It is likely that in favor of improving individual privacy, the definition will expand rather than contract. This has interesting implications for providers that currently do not necessarily have to do much for current regulations. For instance, if an ISP that facilitates cross-Atlantic communication were to be considered a data processor and have to follow all GDPR regulations, the service provided would lower in quality. In addition, if such a definition were given in a country wishing to violate privacy, it could have a cascading effect on privacy as transmissions could become fair game under this legislation.

6.3 Maladaptive Legislation

Privacy regulation will not always be employed in the peoples' favor. For instance, there is and will continue to be legislation that essentially does nothing, but seeks to assure individuals their privacy is protected. This kind of law is generally benign, but helps

providers prevent the implementation of future legislation that may actually yield an impact.

Far more negatively impactful is weaponized legislation. The DPA is a primary example of this. On paper it seems perfectly fine and beneficial. However, in practice it has only been used to infringe on individual privacy. It would not be possible to assert that this would not happen in the future, and there is little that can be done to prevent it. Providers can and do seek to circumvent this, such as Signal [20]. The use of such applications is likely to expand as oppressive governments become more technically literate and are able to better spy on their own citizens.

7 RELATED WORK

Privacy has long since been a concern, and as such there is a great corpus of research on data privacy. These include research on what is required by current regulations [2], future possibilities for digital privacy [6, 9], overviews of the privacy landscape [11], and more. However, much of this research already belongs to a different era of privacy, as the advent of the GDPR is when digital privacy began to change by necessity. Of the relevant post-2016 research into digital privacy, much of it keeps a narrow focus into one facet of privacy [14, 18]. A subset of this post-2016 research is concerned with the future of the privacy landscape [13].

8 AUTHOR EFFORTS

This research was initially separated into three portions based on time period. The past (pre-GDPR), present (post-GDPR), and the future. In order to determine potential trends for the future, both the past and present must be analyzed. However, such analysis could take some time. This was the basis of the distribution of work. When we initially had four group members, the planned work organization was listed below:

(1) Andoni Gorostiza: Coordinating authors; linking past regulation to present; presentation design
(2) Nabhan Aziz: Modern regulation research; presentation design
(3) Timothy Ford: Past regulation research
(4) Jordan McMillan: Modern regulation research; LaTeX typesetting

However, upon the reduction of the author count to two, the work distribution suffered necessary changes. The new organization is listed below, with the approximate time investment of each author to fulfill that task thus far.

(1) Andoni Gorostiza: Past regulation research; presentation design: 20 hours
(2) Jordan McMillan: Modern regulation research; LaTeX typesetting; presentation design: 40 hours

In this organization there was no need for a coordinating task, as all coordination is simplified and can take place in communication between the authors.

9 CONCLUSION

In this work, we analyzed diverse legislation to discover what makes them up, what differences they possess, their impacts on the world, and why exactly they yielded those impacts. These impacts were related back to the structure of the laws and their structural differneces. This emphasizes the true impact of the differences in legislation, and allows us to come to several conclusions regarding privacy regulation in general.

Regulatory change is driven by extraterritorial protection. There is no legislation stronger than that which impacts providers outside one's own nation. GDPR and PIPL's success compared to the other regulations seen show this to be true. For this reason, it is likely that countries will drift into this style of legislating.

The how of enforcement is key to the improvement of privacy. Laws can be well-meaning and pure, but if not enforced mean nothing. The original or presented meaning of a law can also be twisted to harm privacy.

Lastly, government and location matter greatly for the efficacy of a legislation. Governments such as Zimbabwe's have been seen to reverse the privacy-preserving effects of well-meaning laws. Similarly, California has comparatively little political power on the world stage, and as such the CCPA is limited to impacting providers in the United States. The size and location of the EU enables the GDPR to have great impact, as no service can reasonably assert that it will not be servicing European citizens. Additionally, many providers reside within the EU in a massive variety of businesses, which holds them to unique regulations that better preserve privacy. The same can be said of China with PIPL.

We believe the approach taken to holistically considering legislation to be well-designed. Based on the analyses presented, we believe our predictions for the future of privacy legislation to be likely outcomes. While we should be looking forward to the positives regarding privacy regulations, we must also remain vigilant against its potential weaponization.

REFERENCES

[1] 115th Congress. 2022. S.Hrg. 115-683 — FACEBOOK, SOCIAL MEDIA PRIVACY, AND THE USE AND ABUSE OF DATA. https://www.congress.gov/event/115th-congress/senate-event/LC64510/text publisher: Congress.gov.
[2] Pauline Anthonysamy, Awais Rashid, and Ruzanna Chitchyan. 2017. Privacy Requirements. In *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track (ICSE-SEIS)*. IEEE, Buenos Aires, Argentina, 13–22. https://doi.org/10.1109/ICSE-SEIS.2017.3
[3] California Legislative Body. 2018. California Consumer Privacy Act of 2018. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[4] CNIL. 2021. The sanctioned issued by the CNIL. https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc
[5] CNIL. 2022. Cookies: la CNIL sanctionne GOOGLE à hauteur de 150 millions d'euros. https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros
[6] Alfredo Cuzzocrea. 2014. Privacy and Security of Big Data: Current Challenges and Future Research Perspectives. In *Proceedings of the First International Workshop on Privacy and Secuirty of Big Data* (Shanghai, China) *(PSBD '14)*. Association for Computing Machinery, New York, NY, USA, 45–47. https://doi.org/10.1145/2663715.2669614
[7] Enforcement Tracker. 2022. GDPR Enforcement Tracker. https://www.enforcementtracker.com
[8] European Data Protection Board. 2022. Binding Decision 2/2022 on the dispute arisen on the draft decision of the Irish Supervisory Authority regarding Meta Platforms Ireland Limited (Instagram) under Artible 65(1)(a) GDPR. https://edpb.europa.eu/system/files/2022-09/edpb_bindingdecision_20222_ie_sa_instagramchildusers_en.pdf
[9] Clinton Lanier and Amit Saini. 2008. Understanding Consumer Privacy: A Review and Future Directions. *Self* 12 (01 2008).
[10] Moulis Legal. 2022. Didi fined $1.2B for breaching China's data security laws. https://moulislegal.com/knowledge/didi-fined-1-2b-for-breaching-china-s-data-security-laws

[11] David Lindsay. 2005. An exploration of the conceptual basis of privacy and the implications for the future of Australian privacy law. *Melbourne University Law Review* 29, 1 (2005), 131–178. https://search.informit.org/doi/10.3316/ielapa.200510455

[12] National People's Congress. 2021. Personal Information Protection Law of the People's Republic of China. https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021

[13] Razieh Nokhbeh Zaeem and K. Barber. 2020. The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise. *ACM Transactions on Management Information Systems* 12 (05 2020). https://doi.org/10.1145/3389685

[14] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321

[15] OneTrust. 2022. Search Results: Data Protection Act. https://www.dataguidance.com/search/results?search_api_views_fulltext=data+protection+act&apply_filter=yes publisher: OneTrust.

[16] Parliament and President of Zimbabwe. 2021. Data Protection Act. https://www.veritaszim.net/sites/veritas_d/files/Data%20Protection%20Act%205%20of%202021.pdf

[17] California Attorney General Rob Bonta. 2022. CCPA Enforcement Case Examples. https://oag.ca.gov/privacy/ccpa/enforcement

[18] Iskander Sanchez-Rola, Matteo Dell'Amico, Platon Kotzias, Davide Balzarotti, Leyla Bilge, Pierre-Antoine Vervier, and Igor Santos. 2019. Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control. In *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security* (Auckland, New Zealand) *(Asia CCS '19)*. Association for Computing Machinery, New York, NY, USA, 340–351. https://doi.org/10.1145/3321705.3329806

[19] Security and Exchange Commission. 2021. Amazon SEC Form 10-Q. 2021. https://www.sec.gov/ix?doc=/Archives/edgar/data/0001018724/000101872421000020/amzn-20210630.htm#i5986f88ea1e04d5c91ff09fed8d716f0_103

[20] Signal. 2022. Signal Terms & Privacy Policy. https://signal.org/legal

[21] The European Parliament and the Council of the European Union. 2018. Regulation (EU) no 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[22] Committee to Protect Journalists. 2022. Zimbabwean authorities charge journalist Hope Chizuzu under cybercrime law. https://cpj.org/2022/10/zimbabwe-authorities-charge-journalist-hope-chizuzu-under-cybercrime-law

[23] Lucas Nunes Vieira, Minako O'Hagan, and Carol O'Sullivan. 2021. Understanding the societal impacts of machine translation: a critical review of the literature on medical and legal use cases. *Information, Communication & Society* 24, 11 (2021), 1515–1532. https://doi.org/10.1080/1369118X.2020.1776370 arXiv:https://doi.org/10.1080/1369118X.2020.1776370

[24] ZimEye. 2022. ZIM MAKES YET ANOTHER DATA PROTECTION ACT-RELATED ARREST AS AUTHORITIES INTENSIFY SNOOPING ON SOCIAL MEDIA. https://www.zimeye.net/2022/11/18/zim-makes-yet-another-data-protection-act-related-arrest-as-authorities-intensify-snooping-on-social-media