Dream of Californication: welcome to the Californian Consumer Privacy Act

Willliams, J.; Irion, K.

Publication date
2018
Document Version
Final published version

Dream of Californication: welcome to the Californian Consumer Privacy Act

16 Oct 2018 by Josephine Williams, Kristina Irion on California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act (CCPA), slated to enter into force on 1 January 2020, borrows some cutting edge ideas from the EU and others' privacy regimes while also experimenting with new approaches to data privacy. Importantly, the CCPA envisages an online advertisement market in which business are prevented from "*getting high on information,*" [1] breaches are promptly notified, and consumers are autonomous participants with the ability to sell their data at will. Where the CCPA breaks new ground is in protecting

consumers from retaliation for opting out of the sale of their data. Thus, if it lives up to its potential, the CCPA could catalyse a permanent restructuring of the online data mining business. Our contribution will shed light on the new CCPA and offer some observations in comparing it with EU's General Data Protection Regulation (GDPR).

THE FEDERAL DATA PRIVACY INERTIA

> "Try to steal your mind's elation . . . dream of silver screen quotation"- Red Hot Chili Peppers

In spite of recent grumblings in political Washington following the Cambridge Analytica scandal there is for the time being no expectation that the US government will pass comprehensive federal legislation governing consumers' data privacy. Political willpower to regulate the societal harms of technology at the federal level has long been stalled. Since the 1995 closure of the Office of Technology Assessment, there has been a void in federal oversight over the online collection and sale of data.[2] However, over the last decade, the FTC has stepped in to fill the legislative void by investigating data breaches and privacy concerns. [3]

However, informational privacy is gaining increasing momentum. Recently, the National Institute of Standards and Technology (NIST), an agency housed within the Department of Commerce, announced plans to develop federal guidelines for the protection of consumers' online data. In early October, 2018, Democratic Congressman Ro Khanna, who represents Silicon Valley in the House of Representatives unveiled his "Internet Bill of Rights", a blueprint for federal regulation, which would oblige tech firms to alert users of data breaches, provide disclosure, consent and portability inter alia. If such a federal law were passed, it would override, or *preempt* state regulations, however given deep partisan divisions and the slow pace of regulatory innovation in Washington, the odds of swift federal action currently appear dim.

As Supreme Court Justice Louis Brandeis aptly pointed out in 1932, the states are "the laboratories of democracy". While US senators have been grandstanding – and maintaining the status quo -- California has been early on experimenting with data privacy rules. As retold in a New York Times magazine feature, the creation of California's CCPA is an example of strategic advocacy for change. In 2018, a group of California

residents, shaken by the recent Cambridge Analytica scandal, pressured legislators in Sacramento to pass a law that would give California consumers more control over their personal data. [4] However, rather than put the law into the hands of voters who might have demanded an even more radical restructuring of the online ad industry, the legislature chose instead to negotiate its own version of AB 375 and signed it into law on 28 June 2018. The new law provides a huge leap forward for California's citizens and is considered a game-changer for the nation, creating justiciable rights vested in both consumers and the California Attorney General.

THE 'CALIFORNIA EFFECT'

> And if you want these kind of dreams . . . It's Californication (Red Hot Chili Peppers)

If the state is indeed a laboratory for new ideas, the impact of California's data privacy experiment may be monumental given the state's status as the home to Silicon Valley, one of the world's largest economies, and the second largest state in the US. The positive ripple effect to be gained from California's more stringent

standards, what David Vogel has coined the 'California effect,' refers to the upwards pull higher regulatory standards can exert on an industry as a whole. [5] Researchers, such as Bilyana Petkova, contend that federalism or (state jurisdiction) can create "races to the top" in data privacy by enabling states to act sooner than the federal government and to cross-pollinate among state jurisdictions. Also, the testing of innovative policies at the state-level allows federal legislators to later adopt policies that were particularly successful at the state level.

Even prior to the passage of the CCPA, California has already been a frontrunner in driving certain particular data privacy policies. In 1972, Golden State voters amended their constitution to include the right to privacy as an "inalienable right". In 2003, the California Online Privacy Protection Act (CalOPPA) became the first major consumer data handling law in the United States. CalOPPA focused on the availability of privacy policies, compliance with protective Do Not Track (DNT) settings, and the safe storage of consumers' data. In 2005, the "Shine the Light" law was enacted to protect California consumers' private information by requiring transparency and the disclosure of the

identity of third parties receiving consumers' data. [6]

In a sign of its responsiveness to the evolving privacy needs of the digital marketplace, California has taken the lead among US states in regulating the mobile app economy. In 2012, the Attorney General of California and six leading app stores struck an agreement to strengthen privacy protections on mobile apps. By ensuring the inclusion of privacy policies in mobile apps catering to a California audience, the mobile privacy deal was credited with creating positive ripple effects beyond California and throughout the app ecosystem. Similarly, the CCPA may also effectively raise the bar for data privacy protection for non-California residents.

CALIFORNIA'S ELECTRONIC JURISDICTION

> Space may be the final frontier but it's made in a Hollywood basement" (Red Hot Chili Peppers)

The CCPA protects only California residents (humans, not companies) and solely in their role as consumers in a commercial setting. [7] Like the European GDPR, the California law relies on the underlying logic that individuals' data

should be protected according to the whereabouts of the individual supplying the data. Thus, the CCPA applies to businesses around the whole world as long as they reach out to California residents who are present in their state. This means, for example, a California resident, living in Los Angeles whose data is sold by a business in India to a business in Canada would have justiciable rights under the CCPA.

Whilst the CCPA only gives protection to California residents, in practice, the CCPA's California jurisdiction is likely to raise the bar for users outside of California. The CCPA explicitly states that businesses are free to market their online goods and services to non-California residents without providing opt-out buttons or abiding by the CCPA's disclosure requirements. However, it will be difficult to disambiguate data attributable to California residents from residents of other states. The administration cost associated with maintaining separate websites for California traffic is likely to cause many businesses to simply raise their data privacy standards for all users.

THE SCOPE OF CCPA

Personal data: The CCPA gives as broad a coverage to personal information

as the GDPR. Any information capable of being linked indirectly or directly to a particular consumer or household is protected. Also similar to the GDPR, the CCPA covers both electronic and offline data physically given to companies.

Businesses covered: The CCPA is intended to govern heavy hitters: it applies to big data brokers, not small and medium size enterprises and nonprofits. CCPA regulated businesses must be for-profit firms either making over $25 million in annual revenue, or businesses holding the personal data of 50,000 people, households, or devices; or businesses that gain at least half of their revenue from the sale of personal data.

Business purpose exception: Most internal collection and use of data can be shielded from opt-out under the so-called business purpose exception. Generally**,** businesses need not seek consent for one-time transactions such as payments with a credit card and interactions in which the data is not sold or retained or where the data collected does not meet the definition of personal data. Also, the CCPA does not envision an end date for the internal use of data, enabling businesses to hold consumers' personal information indefinitely. By contrast the GDPR regulates all instances

of personal data processing irrespective of whether it is internal to an organisation's business or involves personal data shared with third parties. However, as explained below, CCPA protected consumers will have the right to disclosure of their data collected for a business purpose.

CCPA'S IMPACT

> This is what you're craving . . . Californication (Red Hot Chili Peppers)

Gone are the days when California consumers unwittingly forked over their personal information to powerful tech platforms only to lose track of their data when it was sold further on. The CCPA empowers consumers to say no to the *sale* of their own data. By contrast, the EU's GDPR approaches data privacy from a comprehensive human rights framework, offering a high level of protection throughout the lifecycle of residents' personal data from the moment of its collection, in relation to each use and until its eventual deletion. Still the CCPA improves transparency, allowing consumers to obtain a portable copy of their data and to discover who is holding which of their data, and for what purpose.

One feature unique to the CCPA is a provision that protects consumers from retaliation if they opt out of the sale of their data. For instance, prior to the CCPA, a person wishing to use online map navigation could be left stranded if they declined the business full access to their personal data. After the CCPA, businesses may no longer downgrade the level and quality of services simply because a consumer has opted out. Another exciting innovation is the law's financial incentives that encourage businesses to compensate consumers who wish to sell their data.

The major market shift brought by the CCPA resides in the autonomy it restores to consumers. California consumers will now have full 'ownership' over their own data, with the right to sell their data should they so choose. Before the advent of the CCPA, consumers eager to access the basic infrastructure of the online world had to sign away their data without even realising the value of the personal data they gave up. That dynamic changes radically under the weight of the CCPA, which specifically mentions the right of businesses to pay for the collection of consumers' personal information. In sum, while platforms are prohibited from downgrading consumers, the CCPA encourages

practices that allow consumers to monetise their data. This provision is a laudable step toward strengthening consumers' bargaining power vis-à-vis platforms and raising awareness among consumers of the existence of the data market.

THE NUTS AND BOLTS OF CCPA

> It's understood that Hollywood / Sells Californication (Red Hot Chili Peppers)

What follows is a primer on CCPA's most prominent features, which taken together, aim to restructure power asymmetries in the collection, sharing and control of personal information.

Verification of consumer identity: The CCPA requires that only verifiable requests for the disclosure of a consumer's data be honoured. In practice verifying a consumer's identity will not be very complex. The CCPA is generous toward consumers in its definition of verifiable requests. Businesses must treat requests coming from password-protected accounts maintained by a consumer and made while the consumer is logged-in as verifiable.

Data requests: Somewhat mirroring the EU's right to access, California consumers may in 2020 request a record of the types of data a business holds on them, including information about "business use" and third-party sharing of their data. Businesses are to provide portable information that can be readily transmitted to another business.

Disclosure: Businesses will have to inform consumers of the data they are collecting from their interactions. Disclosure must include the types of data sold, purpose for its use, and the identity of the third party recipients. Notably, while the business purpose exception precludes consumers from controlling businesses internal processing of their data, the disclosure provision does allow consumers to discover which of their data businesses have collected and stored for a business purpose.

Right to 'Deletion': Akin to Europe's "right to be forgotten," California consumers may now request erasure of their information. Businesses must inform consumers of this right. This right, in combination with the disclosure of data held for internal use, may serve as a strategic counterweight to the business purpose exception. Consumers may request to know which of their

personal data a business is storing and then request to have it deleted. However, businesses may use a number of exceptions to escape compliance with deletion requests, including completion of a transaction, cybersecurity, debugging, research, free speech, and some internal analytical use. Sadly, the analytical use exception could make it extremely difficult for a consumer to get personal data stored for internal use deleted.

'Right to Say No² to data sale (opt-out): In a dramatic shift, businesses will now have to obtain consent from consumers -- at or before collection – for the sale of their personal information. Under the CCPA, consumers may, at any time, exercise their right to decline consent to the sale of their personal information. Importantly, the CCPA appears to remedy much of the shortcomings of consent boxes by requiring businesses to place a "Do Not Sell My Personal Information" button on their websites. The button may be a good fix for design issues with opt-out box ticking.

Children's data: Furthermore, the sale of children's data will require express opt in, either by the child, if between ages 13 and 16, or by the parent if younger than

that.

Third party liability: The CCPA creates third party liability when "service providers" and "third parties" processing data violate consumers' data privacy by failing to obtain consent for commercial sale of data or failing to make disclosures of data breaches. This could become a very important measure to counter the murky practice of third party tracking online.

Sanctions: While the CCPA is strong on consumer autonomy, it seems weak on statutory relief for individual consumers. Failure to address an alleged violation within 30 days could lead to a $750 fine per consumer and per incident or actual damages, whichever is greater. This $750 per person fine seems laughable compared to the GDPR's whopping 4% of global turnover. Individuals are unlikely to exercise their right to sue under the CCPA if they only stand to gain $750 as a result. Legislators could have better served individual consumers by creating a higher threshold for fines in an action brought by a single person.

On the other hand, the $750 fine could have a strong deterrent effect on aggregate. Class action suits brought by individuals or the Attorney General could

make the CCPA put its money where its mouth is. For instance, if one-third of California's population of 39.5 million people were subject to an undisclosed data breach, the Attorney General would be able to wrestle back up to about $10 billion. Still, to give the CCPA any teeth, the Attorney General of California will have to settle on a definition of "per violation" that covers each discrete usage of a person's data per instance. It is important to note, however that the $750 statutory fine is not the only available remedy for a violation of the CCPA. Judges may impose any relief the court deems proper, including punitive damages in amount high enough to deter repetition of the violation in the future.

NON-DISCRIMINATION FOR EXERCISE OF RIGHTS: A BIG WIN FOR CONSUMERS

> Firstborn unicorn . . . dream of Californication (Red Hot Chili Peppers)

A major problem with data privacy regulation is the idea that businesses may pull back their services under the pretext that compliance is too costly. The CCPA resolves this risk by protecting consumers from being denied goods or services or charged differential prices simply because they have opted-out of

the sale of their data. In essence, businesses may not punish consumers with higher prices or lower quality simply because they exercise their rights under the CCPA.

Yet there is a risk that this strong non-derogation guarantee may be subsumed by the exception that follows it. The provision that follows states that businesses may in fact offer variations in level or quality of their online goods and services as long as they can prove that the consumer's data is germane to the added level of service. Hopefully this exception will be interpreted narrowly or removed entirely. For instance, a consumer who chooses to give a business her phone number may be contacted by the company via telephone to ensure she is happy with the service while a consumer who opts out of sharing this data may not receive customer service over the phone. Clearly this exception, if interpreted too liberally, risks undermining the guarantee that customers will not lose quality if they opt-out. It is therefore foreseeable that this exception will either be amended, scrapped or litigated after 1 January 2020.

PRIVATE RIGHT OF ACTION FOR CONSUMERS

> Is it war you're waging? (Red

> Hot Chili Peppers)

Consumers may bring individual or class action civil lawsuits under the CCPA in cases of negligent data breach. [8] What looks revolutionary from the outset, unfortunately appears to erect cumbersome barriers to consumer redress. For instance, consumers must wait 30 days to see if a business in violation can "cure" the breach. If within these 30 days, a business is able to show it has remedied the problem and if it provides the consumer an assurance that "no further violations shall occur," then the consumer must desist. Also, consumers must defer to the Attorney General, to see if the Attorney General wishes to prosecute on its own initiative before filing suit.

It is also unclear how the Attorney General will accomplish the Herculean task of auditing the use of data outsourced to "service providers" under the guise of the business purpose exception. [9] While the Attorney General is a formidable prosecutorial authority, its competence is spread over both criminal and civil law. Furthermore, funding for CCPA prosecution is to come directly out of the fines garnered from successful prosecutions of data privacy violations. It is therefore likely that the

Attorney General of California will lack the level of resources allocated to European Data Protection Authorities that have been specialising in data privacy discipline for years.

CONCLUSION

> Destruction leads to a very rough road, but it also breeds creation. (Red Hot Chili Peppers)

By shining a light on the collection and use of data, requiring consent for data sales, and giving greater autonomy to consumers, the CCPA is the most remarkable achievement in US data privacy law to date. The CCPA's opt-out provision makes consumers captains of their own ship rather than unwitting stowaways at the mercy of powerful platforms. However, the law still contains a number of potential loopholes that need shoring up. For instance, the Attorney General must still address the law's administrability problems, the need for a sharper definition of business purpose, inadequacy of individual fines, the question of how businesses approach the positioning and prominence of "Do Not Sell My Personal Information" buttons, and vagueness in the non-discrimination protection.

Yet despite these shortcomings, the CCPA overcomes the highest hurdle standing in the way of data privacy: it creates demand for rights among consumers. Consumers cannot take control of their own data if they do not know they are entitled to it. The "Do Not Sell My Personal Information" button cleverly nudges consumers toward exercising their rights by reminding them that their data is in fact being sold at the same time that it instills a sense of ownership over one's personal data where there previously was none. The law's incentivising financial compensation in exchange for consumers' sale of their personal data is also helpful. One can only hope that over time the sense of entitlement to personal data rights becomes entrenched such that consumers refuse to bear the burden of big data's most pernicious negative externalities.

The CCPA's proponents must be applauded for accomplishing what until very recently looked like an implausible California dream. The new law is in many aspects weaker than what is mandated under the European Union's GDPR but it is not creating conflicts of laws for transatlantic businesses. In fact it is an interesting new lab to observe whether the excesses of today's online

tracking panopticon can be squeezed for good between the GDPR and the CCPA. Both instruments share the principle dilemma of leaving consumers to micro-manage their data privacy preferences which is another form of non-gratified labour. This necessarily places individuals at a strategic disadvantage because rights need to be exercised to come to life.

Footnotes

1. As with the title we are borrowing some lyrics from the Red Hot Chili Peppers song “Californication”.

2. See Richard Solove (April 2010). "Reinventing Technology Assessment: A 21st Century Model" (PDF). Woodrow Wilson International Center for Scholars. Retrieved 2010-05-05.

3. See Hoofnagle, C. (2016). Federal Trade Commission Privacy Law and Policy. Cambridge: Cambridge University Press. doi:10.1017/CBO9781316411292

4. See https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html

5. Following *Vogel, David (1995). Trading Up: Consumer and Environmental regulation in a global economy. Harvard University Press.*.

6. Shine the Light mandated disclosure of a business’ privacy policy as well as the identity of the third parties accessing consumers’ information. See https://www.epic.org/privacy/profiling/sb27.html

7. To qualify as a California resident, a person must be in the state for other than a temporary or transitory purpose, or be domiciled in the state while temporarily outside the state.

8. Data breach is defined as unauthorised access and exfiltration, theft or disclosure due to a failure on the part of the businesses to maintain reasonable security procedures

9. The CCPA makes a distinction between on the one hand “third parties” which purchase consumers’ data and on the other hand “service providers” subcontracted to serve a data processing for a business purpose.