LEWIS SILKIN

Aaaaand… GO! The CCPA has already kicked off but I still have compliance questions!

Despite being a month into the California Consumer Privacy Act ('**CCPA**') 'going live', businesses all over the world are still scratching their heads wondering 'where on earth did these new laws come from and how do they affect me?'

As recently as midway through 2017, a comprehensive Californian privacy law was nothing more than an idea in Alastair Mactaggart's head. The unlikely privacy activist and millionaire real estate developer's ground-breaking Californian privacy ballot initiative was the driving force behind the California state legislator's speedy drafting and signing into law of the CCPA, striking a deal with Mr Mactaggart to legislate the CCPA in exchange for his withdrawal of his ballot initiative.

With the CCPA **already operational**, and enforcement from the state Attorney General action due to commence from 1 July 2020, some UK and EU businesses already fatigued after their GDPR preparation now potentially face another privacy compliance mountain to climb.

Draft CCPA regulations that will be vital for clarifying aspects of the CCPA (and will also impose additional obligations of their own) have only just closed for public comment and are not expected to be finalised until Spring 2020.

You'd be forgiven for having some burning CCPA questions that still need answering, and you wouldn't be alone.

My UK/EU business is located far from the warm sun and sandy beaches of California. Does the CCPA apply to me?

The CCPA will apply to personal information you collect about California residents if you are a for-profit business, '**doing business in California**' and meet any of these threshold requirements:

- you have an annual gross revenue in excess of US$25 million (worryingly, it is unclear whether the revenue threshold applies at a group level or individual level, and whether it refers to California derived revenue, US revenue or worldwide revenue);
- you annually buy, sell, receive, or share for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or
- you derive 50% or more of your annual revenue from selling consumers' personal information.

It does not appear necessary for a business to be physically located in California to be caught by the laws and unfortunately the CCPA is ambiguous on this point also. A UK/EU-based business may be 'doing business in California' if it transacts with California residents, employees people in California or has some other connection to the state.

In addition and importantly, **if you are a UK/EU parent company or subsidiary sharing the same branding as a related company who is themselves caught by the thresholds and criteria above, you will be caught by the CCPA** even if you yourself do not meet the thresholds.

A very narrow (and potentially complex and unhelpful) exclusion from the CCPA applies if every aspect of the commercial conduct takes place wholly outside of California, meaning that the business:

- collected the information while the consumer was outside of California;
- no part of the sale of the consumer's personal information occurred in California; and
- no personal information collected while the consumer was in California is sold.

In summary, just because it is the **CALIFORNIA CPA** does not mean it can be ignored by UK/EU companies. Even those companies without any corporate nexus at all to California will need to undertake, at least, a summary analysis to work out if they are within the scope of the law.

I've been told the GDPR is the 'gold standard' of privacy laws, how does the CCPA compare?

Some of the core features of the CCPA are comparable to the GDPR. We've set out below some of our main observations in summary:

	Main observations	Key differences to the GDPR
Coverage and scope	The CCPA can likely apply extra-territorially, however the extra-territorial provisions of the GDPR are far clearer.	• The CCPA has minimum thresholds which will exclude smaller, non-data driven businesses. • Non-profit businesses are also excluded. • Only California residents are covered, whilst the GDPR covers 'identified or identifiable persons' in the UK/EU regardless of UK/EU residency. • California based businesses do not need to comply with the CCPA in respect of people located in other countries (i.e. there is no 'establishment principle' as in the GDPR). • For one year following its commencement, the CCPA will not apply (save in relation to its notice provisions) to information belonging to job applicants, employees, business owners, directors, officers, medical staff, or contractors. It is unclear whether this exemption will be extended.
Transparency	The right to be informed is a core feature of the CCPA. Both regimes specifically set out the information that must be provided in a privacy notice.	• Businesses are required to communicate updated versions of their privacy notice if they collect additional categories of data or use existing data for new purposes (and slightly bizarrely, according to the draft CCPA regulations, the consumer needs also to provide explicit consent to this additional processing). • Transparency requirements apply to personal information disclosed or sold in the previous 12 months only, rather than all data held.

	Main observations	Key differences to the GDPR
Individual Rights	Access, erasure (deletion) and portability rights are broadly similar to the GDPR. Both regimes require businesses to have mechanisms in place to respond to rights requests and must verify the identity of the requestor before acting on the request.	• CCPA provides no right to rectification of data, restriction of processing, or to object to processing or automated-decision making. • Businesses have 45 days to respond to a rights request which may be extended by either 45 or 90 days where reasonably necessary (these alternate timeframes appear to be contradictory and are likely to be a CCPA drafting error). • Consumers may only make most rights requests a maximum of twice a year and (save for deletion) only in relation to data collected within the previous 12 months. • Businesses must make available two methods for submitting rights requests including a toll-free telephone number (an exclusion applies for exclusively online businesses who have a direct relationship with their consumers).
Security	The GDPR and CCPA are broadly similar in their approach requiring reasonable or appropriate security measures.	• The CCPA does not directly impose security obligations but instead provides consumers with a right to recover statutory damages where appropriate data security standards (based on existing California security law) are not maintained and a data breach results.
Vendors	'Service provider' under the CCPA is a broadly similar concept to 'data processor' under the GDPR. A service provider must be engaged pursuant to a written contract containing mandatory content.	• There are no legal obligations imposed on 'service providers' under the CCPA, save for indirect obligations imposed by the requirement to have a CCPA compliant contract with the business.
Penalties	Due to drafting ambiguity, it remains to be seen how penalties will be administered under the CCPA. However the CCPA has the potential to provide penalties in excess of the GDPR maximums given that there are no applicable caps, and fines are issued 'per contravention' (potentially meaning 'per contravention, per data subject').	• Civil fines can be issued of between $2,500 and $7,500 per contravention. • Consumers subjected to security breaches may recover damages per consumer, per incident of between $100 and $750 or the cost of the actual damages, whichever is greater. • The private right of action re: security breaches and propensity of US citizens for commencing litigation (when compared to the UK/EU) might provide for greater extra-territorial enforcement than the EU's regulators currently have capacity for in respect of the GDPR.

In addition to the differences listed above, there are also novel concepts under the CCPA which don't exist in the GDPR such as:

- An express prohibition on discriminating against a consumer who exercises their rights under the CCPA.
- Businesses which 'sell' (an incredibly wide definition: ranging from exchanging money broadly covering genuine 'selling' of information to even just 'transferring' it) personal information to third parties are required to provide a clear and conspicuous 'Do Not Sell My Personal Information' link on their website homepages.
- Unlike the GDPR which requires controllers to identify a lawful basis upon which to process data (consent, contract, legal obligation, legitimate interest and others), the CCPA has no such requirement (save for requiring consent to sell information once the business has been asked by a consumer not to).

Surely my extensive GDPR compliance efforts do date mean that I'm now CCPA compliant?

Not completely (for example, the requirement for a 'Do Not Sell My Personal Information' link/button!). However, the CCPA is based on many of the same principles as the GDPR (and in fact most new privacy laws globally have many of the same core features, aims and principles). As such, many of your GDPR compliance efforts should help towards your CCPA compliance efforts. The following UK/EU GDPR compliance efforts should help towards fulfilling CCPA requirements:

Mapping exercises and data audits	A business that has mapped and understands its data flows will be best placed to determine whether the CCPA applies and to comply with applicable CCPA obligations. Some additional audits and mapping of data flows may need to be undertaken to address aspects of the CCPA that are different. For instance, personal information under the CCPA can cover information relating to a household rather than being restricted to individuals so further mapping may be required.
Existing privacy notices	Many of the CCPA privacy notice content requirements should already exist in a GDPR compliant privacy notice.
Rights response processes	Established procedures, protocols and automated mechanisms to track and respond to data access and other rights requests maybe able to be used to respond to CCPA rights requests with only slight modifications.
Vendor contracts	Broadly similar content requirements to the GDPR mean that existing data processing agreements may be able to be used as a base to draft CCPA 'service provider' contacts.
Information security efforts	All of your GDPR information security efforts should go towards complying with the CCPA's information security requirements.
Security incident protocols	Whilst the CCPA doesn't introduce additional breach reporting obligations to those already existing in California (the first data breach notification regime in the world), the private right of action for consumers to obtain statutory damages means that businesses need robust protocols in place to identify and contain data incidents and mitigate the risk to the individuals affected. Any GDPR data breach protocol should assist in this regard.
General data protection governance	All actions you have taken in this sphere should go towards demonstrating your compliance with the CCPA. For instance, if you have appointed data champions to lead privacy compliance throughout different business units, you have an internal framework of data protection policies, and you conduct regular employee privacy training and awareness campaigns, these should all be helpful in your CCPA compliance efforts (along with future compliance efforts for other US state laws or other new laws globally).

The CCPA is live. Where should I focus my CCPA compliance efforts?

First and foremost, **verify with certainty whether your company is subject to the CCPA**. If you fall outside of the CCPA's scope, you need not proceed further (but should monitor this in future in case your organisation pivots towards 'doing business' in California).

If you are covered by the CCPA either directly or indirectly (e.g. via the co-branding rules), then there are really three key initial compliance actions to take:

- Ensure your privacy notices meet the CCPA requirements.
- Determine whether you 'sell' personal information as this triggers rights and obligations. As mentioned above, the definition of 'sell' is much broader that its plain English meaning. There are simple steps you can take to quickly reach a level of compliance. For instance, the absence of a 'Do Not Sell My Personal Information' on the website of a business which clearly sells personal information would be a significant breach that the California Attorney General (or Californian data activists) might target for initial enforcement action.
- Finally, identify your compliance gaps and prioritise your compliance efforts using a risk based approach. Areas where non-compliance significantly exposes you to fines or statutory damages should take priority.

I'm still in the dark about my obligations and worried I'm not in compliance

The speed at which the CCPA was drafted and passed into law has left obvious inconsistencies and ambiguities that will be up to either the legislators or the courts to clarify. In contrast to this, privacy law in Europe is highly developed and leaves less room for uncertainty as to interpretation. Despite the GDPR being cutting edge legislation, it evolved from the EU Data Protection Directive 95/46/EC, which itself evolved from a 1981 treaty regarding the protection of individuals with regard to automatic processing of personal data. This all means that privacy compliance efforts in the UK/EU have gradually evolved over time and previous compliance standards have shed light on the likely future compliance standards expected under new privacy regimes (such as the GDPR).

The CCPA on the other hand is not an evolution of an existing Californian data privacy regime. It contains new concepts never before tested or interpreted by courts or enforced by regulators. It has commenced operation at lightning speed and (whilst not yet enforcing the law) the Attorney General expects the law to be complied with from now.

Those struggling to comply with California's novel obligations may be reassured by the words of California's Attorney General stating that he would 'look kindly' on businesses that demonstrate an effort to comply. Where uncertainty or ambiguity means that there is no clear path to CCPA compliance, we recommend doing something rather than doing nothing and crossing your fingers in hope that the California Attorney General, regulators and courts 'look kindly' on your efforts.

Lewis Silkin LLP partners with specialist data & privacy law firms in the United States (and around the world). If you would like more information on the requirements of the CCPA, please contact us.

For further information on this subject please contact:

Alex Milner-Smith
Partner
T + 44 (0) 20 7074 8196
alexander.milner-smith@lewissilkin.com

Bryony Long
Managing Associate
T + 44 (0) 20 7074 8435
bryony.long@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1234
www.lewissilkin.com