wiley

An Introduction to the California Age-Appropriate Design Code

Wiley Connected
September 21, 2022

On September 15, Governor Newsom signed the California Age-Appropriate Design Code Act (ADCA) into law. The bill – which is modeled after the UK ICO's code of practice for age-appropriate design – will impose broad new requirements on businesses that provide an online service, product, or feature that is "likely to be accessed by children." The law will require significant operational changes for any company subject to its requirements. Joan Stewart and Tyler Bridegan of Wiley are joined by Emily Jones of UK-headquartered international law firm Simmons & Simmons to discuss the ADCA and lessons U.S. businesses can learn from the UK Code.

Transcript

Joan Stewart Welcome to the Wiley Connect podcast. I am Joan Stewart, Of Counsel in Wiley's Telecom, Media & Technology group, and today, along with my colleague Tyler Bridegan, we are joined by Emily Jones, a partner in UK-headquartered international law firm Simmons & Simmons' Digital Business team. Emily is a UK-qualified lawyer and has spent over five years in Silicon Valley advising U.S. technology companies on data privacy and security issues. She recently joined Simmons to set up their new office in Silicon Valley. Tyler, I will hand it over to you to kick off our conversation today.

Tyler Bridegan

Related Professionals

Joan Stewart
Partner
202.719.7438
jstewart@wiley.law

Practice Areas

GDPR and Global Privacy
Privacy, Cyber & Data Governance
State Privacy Laws

Thanks, Joan. Today we will explore several elements of the California Age-Appropriate Design Code Act, or the ADCA, which was signed into law by Governor Newsom on September 15, 2022. The ADCA is based largely on the UK ICO Code of Practice for Age-Appropriate Design, which took effect about two years ago. The ADCA represents a wholesale change for U.S. businesses that offer online services or products that may be accessed by children and teens. In adopting the ADCA, the California legislature explicitly noted that U.S. businesses may look to guidance and innovations resulting from implementation of the UK code. Therefore, we greatly appreciate Emily Jones joining us today to provide insight into how businesses subject to the UK code have implemented its requirements.

Emily Jones

Great. Thank you so much, Joan and Tyler. It's lovely to be here and to be talking and sharing insights on such an interesting topic.

Tyler Bridegan

Thanks, Emily! So, let's first talk about the threshold of the two laws. The ADCA will apply to a business – as defined in the California Privacy Rights Act – that develops or provides an online service product or feature likely to be accessed by a child. Joan, how should a business be prepared to evaluate what is likely to be accessed by a child?

Joan Stewart

Thanks, Tyler! Great question. So, this standard casts a much wider net than U.S. companies currently face under the Children's Online Privacy Protection Act or COPPA, which is the federal law that governs how a business may use children's data. So first, before we get into accessibility, let's talk about the definition of a child under this act. A child under the ADCA is an individual under the age of 18 – a significantly higher threshold than COPPA or even the CCPA, which both define a child as under the age of 13. And although it implements its higher age standard, the act does not contemplate a one-size-fits-all approach for children under the age of 18 – rather, businesses must take into account the needs of different age ranges of children. So, for example, design and accessibility may be evaluated differently for a child between the ages of 0 and 5 than for those in the 13- to 15-year-old range.

Okay, so now let's turn to that "likely to be accessed" threshold. So again, this is a higher standard than COPPA. COPPA is triggered when you have an online service that's directed to a child or when the business has actual knowledge that they are collecting information from a child. So clearly any product or service that's subject to COPPA will have to meet the ADCA standard, but beyond that, the ADCA sets out elements that a business should consider when evaluating whether or a product or service is likely to be accessed by a child.

And these include if there are advertisements that market to children; there are design concepts that appeal to children, such as games, cartoons, music, celebrities popular with children; when the company has internal research that indicates that a significant amount of the audience is children; or when it's based on reliable evidence of audience composition, so, your analytics that the product or service is routinely accessed by

children. So, businesses are, of course, running analytics on the use of their online products and services, and under the ADCA, they really need to be paying close attention to what those analytics reveal about user demographics.

It is incumbent on companies and especially legal and privacy and compliance teams to be engaged with their marketing and analytics folks to really understand who's using your products, services, or even certain features of those products and services. So, bottom line here is the threshold is very broad and likely to sweep in more products, services, and features than were captured by COPPA, and despite the elements set out in the act, the standard still seems very vague and will require some careful evaluation by businesses.

Tyler Bridegan

So, Emily, turning to the UK front, does the UK code have the same threshold, and how have UK businesses interpreted this standard?

Emily Jones

Yeah, that's a really interesting question, Tyler, and, you know, given that we know that the AADC has been modeled on the UK Code for Children, then not surprisingly, it's a very similar position in the UK.

So, in the UK, the code applies to providers of online products and services that process personal data and are likely to be accessed by children in the UK, so again, it's a much broader definition. It means that companies may be caught by the code even when they're providing services which are not specifically directed to children under 18. The code gives a bit more guidance about what this could mean and says, basically, that if there's a possibility of services being accessed – and that's more probable than not – then UK businesses should really look at those services in more detail and then take appropriate steps.

Again, on the same lines, the same kind of things that Joan mentioned: Are they likely to appeal to children? Is there an identifiable user group under 18? And then, businesses are expected to carry out an assessment and keep records around that. And many UK businesses have assumed that they are going to be covered by the code and that their services will be accessed. I think the challenge is for companies that are in a somewhat of a gray area where they are not 100% certain, but it's hard to rule out completely. So that's where we've been seeing a lot of work by companies to carry out some assessment.

Tyler Bridegan

Very interesting. So, turning to the obligations that ADCA imposes, several such obligations on covered businesses, including that the business estimate the age of a child user with a reasonable level of certainty appropriate to the risk from the business data use practices. So, Emily, how does the UK code require a business to estimate a user's age? Can you share with us how UK businesses have implemented this requirement?

Emily Jones

Yeah, sure, so age assurance is a really important aspect of minimizing and assessing risk to children. But it's been a particularly challenging aspect of the code to implement, especially because companies are looking to balance the kinds of information they might collect to make decisions or be certain about age versus compliance with other parts of the Children's Code and, of course, GDPR and the Data Protection Act around data minimization. And in fact, there was a lot of discussion about this in the run up to the code effectively being enforced, and so the ICO issued some specific guidelines on age assurance in October 2021, which I recommend that people have a look at. There's a lot more in those guidelines around what methods can be used, and, really, it all depends on risk.

If there's a high risk to children, then they would expect companies to take steps to be more certain around age – for example, using hard identifiers to verify age or third-party services. And if there's a lower risk to children, then estimating ages, such as age ranges, using self-declarations, or using existing account holders to verify the age of users, or other technical measures, such as monitoring behavior on a site, would be more appropriate. But again, the real theme here is keeping records, documenting assessments, demonstrating an approach to make sure that there's the relevant evidence if the ICO requests it.

Tyler Bridegan

So, it seems that in order to estimate a user's age, a business may need to collect some additional information about a user. Joan, what restrictions are placed on what a business can do with that information?

Joan Stewart

So, yes, under the ADCA it may, in fact, be necessary to collect additional information – as Emily notes, there are other options businesses may want to explore to estimate a user's age. But the ADCA does allow a business to collect information that is not otherwise needed to use a product or service specifically for that purpose of estimating age or age range of a child. As Emily also notes, that potential need to collect additional information really seems counterintuitive, as the primary purpose of these laws is to reduce the amount of information collected about a child, but for some businesses this may be the most accurate way to estimate age. And, similar to the UK code, under the ADCA, the requirement to estimate age needs to be in proportion to the risk of a business's data collection and use practices. So, practices that are riskier under the ADCA – profiling, monitoring, or practices that involve the collection of precise geolocation – are going to require a more precise estimate of age. So, if the business decides to collect additional information, it may only be used for the purpose of estimating age and only retained long enough to perform that age estimate. So, operationally, if businesses are going to use this option, they need to ensure they have a routine data purge set up to make sure this information is being deleted and is being siloed out so it's not being used for any other purpose.

So, businesses currently subject to the CCPA maybe can draw on their experiences implementing the verification requirement for certain consumer rights. So, under the CCPA, you have to collect additional information to verify an identity before honoring certain consumer rights, and you're also restricted from using

that additional information for other purposes, so businesses that have this process set up may be able to build on that to build out that age estimate process for the ADCA. But the key takeaway here is that the collection of additional information to verify age or the age range is an option, but it comes with additional compliance obligations, and if a business uses this option, it needs to make sure that it's not using that information for any other purpose.

Tyler Bridegan

Good to know. So, in addition to affirmative obligations, the ADCA also strictly prohibits certain actions. It seems that one of the more impactful prohibitions is the ban on profiling by default. So, Joan, could you tell us a little bit about that – how the ADCA defines profiling, and what does this mean practically for businesses?

Joan Stewart

Yeah, so this prohibition is really going to impact a lot of businesses, especially, I think, in the advertising space, and it'll probably require the disabling of some features that people actually like about certain online services. So, profiling is defined in part as any form of automated processing of personal information that uses personal information to evaluate aspects of an individual. So, a very technical definition, but it includes, among other things, analyzing or predicting information about personal preferences, interests, behavior, location, or movement. So, if you've ever gone down, you know, the rabbit hole on YouTube of watching the next video recommended for you, that is profiling.

So, under the ADCA, it is illegal to profile by default, unless the business can demonstrate that it has appropriate safeguards in place to protect a child and either a compelling reason why the profiling is in the best interests of the child, or the profiling is necessary to provide the service and only while the child is knowingly and actively using that service. And then, of course, the user can also choose to enable these features. So, practically, this prohibition is going to impact how businesses approach, among other things, digital advertising and that content optimization algorithm. So, for example, apps that are targeted to kids that use an algorithm to recommend what to watch next or read next would have to disable that feature, unless you can demonstrate that feature is in the best interests of the child or are necessary for the service. So, from a usability standpoint, I suspect we're going to see a lot more pop-ups in our future, as online services ask if we want to enable these features that they will have to have turned off by default.

Tyler Bridegan

So, turning to the UK front, Emily, is profiling defined similarly under the UK code, and how has the restriction on profiling impacted online advertising for UK businesses?

Emily Jones

It is very similarly defined under the UK code, and, in fact, more broadly, of course, this all sits within the GDPR, where there are specific concerns that have been identified for children, especially around profiling. So, as Joan says, there's a similar position in the UK – profiling by default is not permitted, except in limited

circumstances. There would need to be a compelling reason. For example, if the profiling was a part of the core service. Typically, online advertising is not part of a core service, and so that is having an impact on online advertising, which is still possible but is just more challenging in accordance with the code and, more widely, GDPR. And, of course, we have an additional layer of regulation, which is the Privacy and Electronic Communications Regulations, which control the use of cookies, which obviously are used in connection with online advertising in many cases. So, I think what's quite interesting is the code does give examples of what acceptable practice might be in the context of profiling, but it really emphasizes the fact that companies need to think very carefully about profiling, the very different types of profiling they might do, and making it really clear to users what exactly that means for them.

Tyler Bridegan

Awesome! So, turning now to enforcement, the ADCA does not have a private right of action. The California Attorney General has exclusive jurisdiction for enforcement, and fines could be as high as U.S. $7,500 per affected child for each intentional violation. The law does currently contain a 90-day grace period to cure violation identified by the AG in certain circumstances. So, Joan, the 90-day cure period is only available in certain circumstances. Can you describe for us what a business needs to do to have access to a cure period?

Joan Stewart

Yeah, absolutely. So, the law requires companies to conduct a data protection impact assessment, or a DPIA, before launching a product. So, the DPIA needs to cover the purpose of the product, potential risks from children using the product, and how the product uses personal information. After completing the DPIA, companies must also document any risk of material detriment and create a plan to mitigate or eliminate those risks before the launch of the product or the service. If the AG asks for it – the California AG asks for it – the company must provide within three business days a list of all the DPIAs it has completed, and, again, if requested, it must provide a full copy of a full DPIA to the AG's office within five business days of a request.

So, the "carrot" here that the act is putting out for businesses is that if you were in substantial compliance with these DPIA requirements, then the AG's office must give you written notice before initiating an enforcement action and allow you a 90-day cure period to address those alleged violations. If you fix the alleged violations within the 90 days and put measures in place to keep it from happening again, the enforcement action won't move forward, so I think that's a significant incentive to take the DPIA requirements seriously. Not only will it make it easier to avoid some significant fines, but you will be in a much better position to cure any violations because, remember, as part of the DPIA process, you have to have already done the work to create a mitigation plan.

So, this act really represents a wholesale change in privacy practices for a lot of businesses. Having the opportunity to cure any perceived violations during, especially, this learning curve period when the law is first implemented, I think will be crucial, and we really encourage businesses to take this requirement seriously and incorporate DPIA into its product development cycle.

Tyler Bridegan

So, Emily, on the UK front, how is the UK code enforced, and have there been any notable active enforcement efforts?

Emily Jones

So, the code is enforced under the umbrella of the GDPR and the Privacy and Electronic Communications Regulations that I mentioned, and so all of the various powers that the ICO has are already set out within those laws. Those include investigating, issuing enforcement notice, warnings. Ultimately, there is a possibility of a fine of up to 17.5 million pounds or 4% of annual turnover. I think it's fair to say that, so far, we have seen the Commissioner focus more on encouraging compliance – ensuring that companies have the tools and information to comply – and also on carrying out audits. So, they have already invited a number of companies, particularly in the games industry, to work with them to carry out audits. That seems to be the sort of approach that they're taking for now, but they've been very clear in their enforcement policies that the protection of children's data is a high priority, and so if companies aren't conforming with the code, they can't demonstrate steps they've taken, then they're going to be at higher risk of a greater level of fine and additional enforcement action from the regulator.

Tyler Bridegan

Good to know. So, that is all the time we have for today. We hope that you have found this podcast informative, and we wanted to thank you again, Emily, from Simmons & Simmons, for taking the time to talk with us. We appreciate your time and your insight into lessons we can learn from the UK code.

Emily Jones

Thank you very much. It's a pleasure to join you today.