UC Berkeley
Center for Law & Technology

Data Subject Rights: What Happens After the Request Comes in Transcript

Wayne Stacy 00:30
So, welcome everyone to the Berkeley Center for Law and Technology's [BCLT] Expert Series webcast. We've got another interesting program for you this week, a topic that, you know, theoretically seems really easy. Data subject rights. We hear about this and the right to forget. But once you scratch the surface just a little bit and you look at issues, operational realities, this is a terrifying area for companies to try to navigate. And I'm really excited today, Ali Jessani, he's counsel at WilmerHale in Washington D.C. has joined us to share some of the real issues people are facing, not just the surface level problems. So, Ali, thank you for taking your time to do this. I know you've got a day job, but this is the kind of information that in house counsel people need to know about before they get in trouble, not after. And so, I appreciate you reaching out to us.

Ali Jessani 01:28
Yeah, absolutely. Happy to be here. Thanks a lot, Wayne, for having me. Excited to do this for Berkeley Law. As Wayne mentioned, our presentation today is about data subject rights, obligations, operational realities, and regulatory expectations, and as Wayne was referencing, again on the surface this seems like an easy topic. It seems like, you know, something that everyone is familiar with at a baseline level. But as someone who deals with this every day and advises companies on this topic, there are complications in terms of how these data subject rights are executed, the types of compliance mechanisms needed by companies to ensure that they're accurately recorded and accounted for, as well as some of the regulatory risk that exists for companies as well. So we'll talk about all of that in today's presentation. So as Wayne was mentioning, I'm Ali Jessani. I'm a counsel at WilmerHale, based in the Washington D.C. office. I advise clients on all aspects of privacy, cybersecurity, and regulatory compliance related to data protection. In particular, of my specific area of expertise is U.S. state privacy compliance, and that's where a lot of these data subject rights questions are arising, and so we'll focus a little bit on that in today's discussion. So, the five questions we're really going to focus on today are: What are data subject rights or DSRs, and what obligations do they create for companies? What laws govern DSRs? What are the challenges and risks businesses face when operationalizing DSRs? How do those obligations vary based on a business's specific context? And how are regulators addressing DSR compliance? So, what are DSRs and what obligations do they create? So, on the surface, these are all things that we've heard of in the past: the right to access, the right to know what personal information is being collected about you, used and disclosed, the right to delete your information, the right to erasure, it's called in some jurisdictions. Related to that is the right to correct inaccurate information, the right to portability, the right to have your data in a usable, transferable format, and to move it from one entity to another. One of the trickier ones is the right to opt out of sale or sharing of

your information, and more recently, the right specifically to opt out of targeted advertising. We're seeing an AI-related right under a lot of data protection laws related to what is called profiling in certain high-risk profiling cases. There's the right to limit the use and disclosure of sensitive personal information. Related to that is the right to opt in to the processing of certain sensitive personal information. So, some laws defer on this issue. Some laws say that you have the right to opt. You are required to obtain an opt in for the processing of sensitive personal information; other laws only provide a right to opt out, and there's a certain ability for consumers to appeal a denial of their rights. There is also a right to not be discriminated under certain data protection laws for exercising your rights. So, you know, you can't be treated differently in terms of being charged more because you're deciding to exercise a right to delete your personal information or right to access your personal information. This is an interesting right because it relates directly to how companies are permitted to implement their loyalty programs, and we'll talk about that in some of the operational concerns we'll discuss. So, what obligations do these rights create for companies? I mean, at a high level, you know, the simple answer is that companies are required to provide consumers these rights, but what that looks like in practice varies, and we'll talk about, you know, where these laws are. But it varies by a number of factors. It varies by, you know, whether there is an affirmative right for a consumer under an applicable data protection law. So currently, 23 states in the U.S. have some form of a comprehensive privacy law that creates an affirmative right, but not all of those states have the same rights. And so, there's a question of what does that right actually exist, and what does it actually mean?

Ali Jessani 06:20
And then when you get a data subject rights request, and, you know, you have every intention of complying for it, it's figuring out okay, well, I, you know, what does it actually mean to comply with the request within this time period that's permitted under the law, and sometimes it means under California, for example, confirming receipt that you've received a request and letting a consumer know that you're working on it. There's also a question of who, what entity does the right actually apply to in a specific context. So, for example, in California, there is the concept under the California Consumer Privacy Act [CCPA] of an entity being what is called a business under the law, which is a defined term, and that definition is really important for understanding what part of a corporate entity a specific request to delete, for example, applies to. So, if you are a business ABC Incorporated and you have multiple subsidiaries that are also co-branded as part of the larger family of ABC Incorporated, you are all the same business for purposes of California, and I'm simplifying a little bit, but just to emphasize that point, what that means is if one part of your business gets a deletion request, you have to effectuate that request throughout the entire business in California, and that could include all of your various subsidiaries, some of whom may not even, you know, be in the same business line. They may not even have a data sharing mechanism between the various entities, but the way the law is structured, the opt out or the deletion request has to occur throughout the business, and so that can be a challenging aspect for companies, especially that are in multiple industries or that have, you know, multiple business lines operating under the same name. And then there's transparency obligations. So especially in a situation where a business is deciding that they want to, that they are not legally required to comply with the request, or they're saying, you know, there is an exemption under the law, or the consumer's request is inconsistent with how the company processes the consumer's data. They have to explain that they're denying that request, which can be burdensome and time-consuming for companies, depending especially on the volume of requests that are coming in recent months from

consumers. And then there are record keeping and training requirements under certain laws, especially in California under the California Consumer Privacy Act.

Ali Jessani 09:06
So I alluded to this a little bit, but we'll talk a little bit about the laws that govern the DSR. The comprehensive state privacy laws are really what are driving some of this discussion. These are laws of what are intended to be laws of general applicability. They're very similar to the GDPR [General Data Protection Regulation] in the EU. You know, In the U.S. we don't have a federal privacy law that is similar to the GDPR that applies in all contexts; what we've had historically are sector-specific laws such as HIPAA [Health Insurance Portability and Accountability Act] for healthcare and the Gramm-Leach-Bliley Act [GLBA] for financial data. We've had use case-specific laws like the Fair Credit Reporting Act [FCRA] for consumer reports, or, you know, context-specific laws such as the Children's Online Privacy Protection Act [COPPA] for children's data, but we haven't had laws that apply in all contexts. So, given the lack of a federal privacy law, a number of states, especially after the GDPR passed, started passing their own comprehensive privacy laws that protect consumers in their own states, and while these laws are intended to be laws of general applicability, they do have exemptions for certain data that's already processed under federal law. So, for example, if you're a healthcare covered entity and you process information under HIPAA, you're exempt from these state comprehensive privacy laws. Similarly, if you're a financial institution processing financial data under the GLBA, you're exempt from complying with these requirements under the state privacy laws, and so again, what this does is create complexity. These laws don't always apply to all entities; they apply in some specific context to essentially the entities that are not already covered by a legal framework governing their data processing activities, and even then, they don't apply to all entities in that context because, I mentioned earlier, for example, the definition of a business in California. There are certain, to be a business in California, you have to meet a minimum revenue or a data processing threshold, and that's similar in all of the other 22 states as well. So if you're, and the goal here is to, you know, not create burdens for small businesses, and so if you're a small business you're not subject to these laws the same way that a larger business is that isn't otherwise exempt from the scope of these laws, so this is generally the framework: these 23 state comprehensive privacy laws. What they are doing is creating affirmative rights for consumers in those states. Now, what we are seeing, though, is that companies that are national companies or multinational companies, for both a business perspective and an operational perspective, it doesn't necessarily make sense for companies to discriminate against consumers that live in states that don't have these comprehensive privacy laws. So, you know, if you're a business that operates nationally, and, you know, you provide these rights to residents in California and Virginia and Connecticut, because those laws, you know, have, those states have these laws. It doesn't necessarily make sense to you from a business perspective to reject those requests from a New York or a Massachusetts consumer who's looking to have their data deleted, because one, it signals, you know, that that you may be viewed negatively from a media and from a reputational perspective for doing this kind of slicing and dicing, but also once you have this operational mechanism in place, it is easy enough for you to exercise these rights, you know, regardless of where a consumer is based, and so even though, again, less than half the states have this right, we're seeing companies adopt a one size fits all approach, though it depends on the specific context and the specific right. So, for example, if you're a business and you say, you know, we're going to give consumers in every state the right to opt out of, you know, the use of their data and targeted advertising, or the right to delete

their data, because, you know, we think consumers everywhere should have that kind of agency in their data as a best practice. You know that may make sense, but at the same time you may say, while we're going to do that, we're not going to get an opt in for sensitive data everywhere because that requires an extra operational challenge. So to emphasize that a little bit more, certain states require affirmative consent prior to a company processing certain categories of data. So this could be health data or racial or ethnic data, other categories of data that are deemed sensitive by a specific law, precise geolocation data, for example, and a company may say, well, for that specific requirement, what we're going to do is only get opt-in consent from consumers that live in a state where they have that affirmative right, and everywhere else we're only going to provide an opt-out because getting an opt-in is operationally challenging a lot of times. Or they may choose to exclude those states altogether because an opt-in is so operationally difficult. We're seeing this a lot in the consumer health advertising industry, where certain states have created real operational challenges to engage in targeted advertising using health data or, health or data, that can be reasonably associated with health data, and so what some companies have done is exclude those states altogether from the scope of where they're operating this business line because getting opt-in consent in a market where you don't necessarily have a direct relationship with a consumer to be able to do that can be, you know, a real, you know, operate not only an operational challenge but an impossibility, and so we've seen, you know, certain states be excluded from that altogether. One of those states is the state of Washington, and that state doesn't have a comprehensive privacy law, but it has what's called a consumer health data law, the My Health My Data Act, which, among other things, creates data subject rights in relation to consumer health data specifically. That term is defined very broadly to include not only things that are traditionally thought of as health data, such as prescription data and, you know, description of health conditions, among other things, but also information that can be derived from or inferred to be health data. So this includes a lot of non-health data that is associated with health data. So, for example, your purchase history of certain foods, for example, may be used to indicate that you have a certain health condition, even though, you know, you're not, the information about the health condition itself isn't what is being reported or being processed. But information about a purchase history that is then being used to infer a health condition may still fall within the scope of that law. So, to bring it back, in addition to the 23 comprehensive privacy laws, we have these consumer health laws that are creating rights for consumers. We're also seeing data broker laws. There are five states now that have some version of a data broker law, and what these states are doing is not only creating additional obligations for companies that are required to register as data brokers, but they're also making it easier for consumers to exercise their rights. We'll talk about that in the California context in a little bit, and then finally, even if you are a company that, you know, is adopting a state by state approach, or choosing, or you fall outside the scope of the comprehensive privacy laws because you're a small business or whatever it may be, you have to still think about the Federal Trade Commission [FTC] and the FTC Act. And so, for example, if you make a statement in your privacy policy that says, you know, we will honor any data subject request we get, regardless of where you are from, and it turns out that you were treating those on a state by state basis, that may be a deceptive statement about how your data processing activities, that is subject to the FTC Act. So that's something that's always in the background: the promises you are making to a specific consumer and how those promises relate to your actual data practices.

Ali Jessani 18:43

So, getting a little bit deeper into the challenges and risks in operationalizing DSR, one of the challenges is, you know, fragmented intake. So, you know, you can imagine for large multinational companies, you know, there are requests that they receive in a variety of forms; they can come by email, by web form. You know, these requests can be, a lot of companies now have formal mechanisms for submitting requests, but these are not always the requests, the mechanisms through which consumers make requests, and so there could be a real disconnect between a consumer thinking that they're making a valid request to a company and that request not being processed by the company because it didn't go through its official channels, and so that creates a potential gap for a company in terms of how it's supposed to respond and whether it's met its obligations in relation to a potential request. There are also new tools and laws that are making it easier for consumers to submit requests. So on the tool side, we're seeing an influx of these both apps and other online mechanisms through which consumers can make accounts and then submit requests to a number of companies at once. So one friction for consumers in this space is that if I'm a consumer and I want every company to stop using my data for targeted advertising, I would you know in the past I'd have to go to each company's website that I've interacted with or potentially interacted with, go to their web form, submit an opt out, and that creates you know this this friction for me as a consumer because of the time consuming activity. But these new tools, what they're permitting consumers to do is they are allowing consumers to make one account, provide their information, and then that tool sends an opt out to 100 or hundreds or 1000s of companies at one time. So again, this theoretically makes it easier for consumers, but what it does for companies is that, one, they get an influx of requests at once; these requests aren't always, and actually most of the time aren't, in the mechanism that is set up by the company to respond to their requests. So, they, you know, they don't have a that you may have a great centralized process for responding to requests and completing them when they are submitted through official channels, but often, when these tools are not, when these requests are not submitted through an official channel, then they get backlogged, or they can get missed, and that creates a real challenge for companies, especially as these requests come at once. Related to, you know, what is both a new tool and a new law: a lot of the new comprehensive privacy laws require companies to honor what are called opt-out preference signals. These are technical mechanisms that consumers can implement through their web browser that indicate to the company that runs the web browser to opt the consumer out of the sale of their information and the use of their information for targeted advertising, and so again, what that does is that if I'm a consumer, I've implemented an opt-out preference signal. I go to the company's website. The company has to have a mechanism for recognizing my opt out and for implementing it. Now, this can be easy enough on the company's end in some cases, and others though it can be quite difficult because, as I mentioned earlier, one of the issues here is who is the entity that is receiving a request. So if I have, you know, a browser and I'm an authenticated user, meaning that I am logged into my account with that company, whatever it may be, and I have an opt-out preference signal enabled, the company not only has to honor my opt-out preference signal in relation to my web browser, and that may be easy, but it also has to apply my opt-out of sale to other contexts where they are selling my data because they know who I am in that context. That may be different for an unauthenticated user who has not signed up in their account, and all the company has in that scenario is a specific IP [Internet Protocol] address or cookie information in relation to that consumer. So again, this is just adding more complication to this overall area. And then finally, in terms of new laws and tools, there is also, for data brokers specifically, California just launched their deletion request and opt out portal through which California consumers can log in, create an account, and opt

out of all of the entities that are listed as data brokers under California's data broker registration law. That law defines data broker quite broadly because it defines the concept of sale quite broadly. So, in addition to companies that are traditional data brokers, companies that you would, that actually practice in the buying and selling of information and compiling information for sale, a lot of the targeted advertising industry, because of how this law defines the word sale, has been, has essentially fell into this data broker registration requirement, and now are required to comply with this new DROP [Delete Request and Opt-out Platform] tool, which again is just making it a lot easier for consumers to exercise opt out and deletion rights, and this is creating challenges for companies throughout the space. There's also incomplete data mapping consideration. So, data mapping is an important concept for companies as part of their overall data hygiene, and the idea is knowing where your data sits in your specific system. If you have incomplete data maps, you're not going to know, for example, how to properly respond to a deletion request, and that creates a risk of non-compliance in relation to specific DSRs.

Ali Jessani 18:43
There are identity verification concerns, and this, where I've seen this particularly play out, is in relation to these new tools that are making it easier for consumers to exercise their rights. You know, a consumer may fill out their information, send it to hundreds of companies at once. But if you're a specific company, for example, that operates in the healthcare context, you may have a specific context or a different email address that you associate with that consumer than the one that they have used to send out this request, and so you may not be able to verify that this is the right consumer, and so, you know, that again creates operational challenges for companies, and this may require some back and forth with the consumer, which both adds to the hurdle required to comply with the request, but also to the timing requirements, which are also relevant in this scenario. There are issues related to vendors and downstream recipients. So, if you're a company and you get the right to opt out of sale under a lot of the laws, it's not just, or the right to, you get a deletion request. It's not only that you are required to delete that consumer's request. You have to flow that request down to your processors, to your vendors that have a consumer's data in that context as well. So again, this adds just another layer of complexity. It adds to the operational difficulty of complying with these requests, especially as many of them come in at once. We've talked already about some of the shorter clocks and some of the timekeeping requirements, as well as the record keeping requirements. I mean, this is an essential element, especially in the event of a regulatory investigation; the standard in these investigations is not often perfection, but having a demonstrable process can often help to show that, you know, the company is doing the right things. But even you intend to do the right things and have the right process, and the process doesn't live up on all particular circumstances, and that can be okay as long as there is a process in place. It just depends on, you know, what the regulator is looking for. And opt out interfaces are also important, not only from a privacy perspective, but there's also a consumer protection element to them, and privacy regulators are focused on those interfaces as they, you know, as they risk potentially becoming dark patterns. So, for example, you know, if you're trying to get an opt in from a consumer to process their sensitive information, you can't only show them, you know, a yes option, or a yes option that's much larger than the no option. You know, this would potentially be considered a dark pattern that violates both the data protection law and the general consumer protection law in that context.

Ali Jessani 20:33

So, thinking more about business obligations, the context of a specific business is really important. Privacy law often distinguishes between controllers or businesses, or, you know, a primary data processor in a specific context, and a processor or a service provider. You can think of this as principal-agent requirements and other areas of law. But the idea is that the principal owns the data protection compliance obligation, and the agent or the processor, the service provider, follows the controller's instructions in a specific scenario. So, what that means is, if you're a processor or service provider, your obligations are primarily by contract, and those contracts may have more specific requirements than what a law requires. Because, you know, if you're a smaller company and you're negotiating with a larger company, you often don't have a lot of negotiating power, and you're agreeing to the larger company's template requirement, which again may be, for example, require you to send, you know, send information about data subject requests within 24 hours of receiving them, even though that's not required by any specific law. You know, you may have to provide very specific information about the data subject requirement. You may have to comply with the requirement yourself. You may have to directly interact with the consumer, even though it's not necessarily your legal obligation to do so. So, it's important to think about what the contract says in a specific context, in addition to what the law says. Sector and data type is also important. As I mentioned earlier, if you are in a regulated industry, if you're, you know, a covered entity or a business associate that processes information pursuant to HIPAA. If you process clinical research information under the Common Rule or financial information or the GLBA, you may not necessarily have the obligation to comply with state comprehensive privacy laws. Where this issue is interesting is in the context of entity-wide exemptions for certain regulations. So, for example, Virginia, for example, not only exempts information process pursuant to HIPAA, but also exempts entities, covered entities, and business associates that are regulated by HIPAA. So to stretch this example, you know, you can be a company that is a business associate in one part of your business, and your business can be four parts. And the smallest part of your business, you otherwise, you know, are a direct-to-consumer company, but you operate one part of your business where you operate as a business associate to covered entities. What that means is, theoretically, you could say you're not required to comply with the Virginia law at all because you're a business associate that's exempt from the scope of the law, even though technically only a small part of your business is regulated by HIPAA. Now, you know, we have seen some regulators, you know, point out the issue with this broad-based exemption, and this exemption doesn't exist under all of the laws, but it could be a way for companies to say they're not legally required to comply in contexts where their compliance might otherwise be expected. And, I mentioned earlier, sensitive data being an area of specific requirements because it often requires opt-in processing, which is, you know, under most of the U.S. comprehensive privacy laws, they are not opt-in regimes; they are generally opt-out regimes. But for sensitive data, a number of the laws are opt-in, do create opt-in requirements, and health data is where this issue is really playing out because some of the laws define health data very broadly, to again include not only data that is traditionally thought of as health data, but also information that could reasonably be associated with health data. It also matters who the individual is. So one of the benefits for companies under most of the comprehensive privacy laws is that those laws exempt data processed in an employment or in a commercial capacity. So what that means is, you know, those the rights that otherwise exist for consumers don't apply to your employees or to your business contexts. California does not include such an exemption. So, in California, you do have to comply with rights in relation to those contexts as well, and so that's an important factor. And then scale and jurisdiction. So, if you're a direct-to-consumer company, you generally have more obligations than if you're a B2B [business-to-

business] company. For the reason I was saying earlier, a lot of the information process in a B2B context is exempt from the scope of the law, and if you're a B2B company, your obligations are going to come from being a processor to your customers, where you're assisting them rather than having primary obligations. If you're a company that is a registered data broker, you have the most obligations because you have obligations under the comprehensive privacy laws, and you have these specific data broker laws that apply to you, and there are tools that are making it easier for consumers to exercise their rights, including the DROP requirements that I discussed earlier.

Ali Jessani 20:33
And then finally, how are regulators thinking about this issue? You know, California has been the, California and Texas have been the only regulators that have brought enforcement actions under their comprehensive privacy laws. For what it's worth, California has two regulators that deal with this issue: both the California AG [Attorney General]'s office and the California Privacy Protection Agency [CPPA] are both, you know, both entities that are regulators that bring enforcement actions under the CCPA. More and more regulators are focusing on this issue. From the limited enforcement actions we have seen thus far, it seems like not honoring opt-outs and not honoring deletion requests or other is an area of focus for consumer complaints. So a lot of consumer advertising to a specific company, and then they'll continue to get targeted ads because their opt-out hasn't been processed. That's an easy way for a consumer to see, hey, I did something and this wasn't adhered to. Let me complain to a regulator about it, and so, you know, that can often be a mechanism for a regulator, especially if they receive multiple complaints against the same company, to follow up with the company, and that eventually could lead to an investigation. It's also an easy thing for a regulator to see on their own end. So, I was mentioning earlier about opt-out preference signals and how this is becoming an area of focus for both laws and regulators. You know, a regulator can go on your website and see whether you're honoring an opt-out preference signal or not. And so, this again is an easy way for a regulator to see. It's essentially low-hanging fruit for a regulator, for which then they can begin an investigation and then look into whether you're complying with other aspects of what the laws require, including training and record keeping, things that are not public, the things that a company doesn't make public, but that can then become part of a larger investigation.

Ali Jessani 36:44
And with that, we can wrap up with key takeaways. You know, the process is what's important for the company receiving a request: verifying individuals, acting across your systems, explaining the outcome, and documenting it. I mean, this is again, these are, this is easier to say and harder to execute. But having things like proper data mapping, having a uniform process, understanding where your obligations are. That's where, you know, that's where the process is really important. It's also important to know that there are timing requirements to these laws, and so it's not enough to, you know, take your time and get to it when you get to it. You know, these laws often require compliance within 45 days, or an extra 45 days if you reach out to the consumer and tell them their request needs additional time. As we talked about earlier, context is really important. So thinking about where your role is, what sector you're in, whether there are exemptions for that sector or for that data type, and whether, you know, a request is actually required to be complied with based on whether the person is acting in a consumer or a B2B or an employment context is also really important. And then regulators are paying attention, and having a documented, demonstrable process is really important because, again, the process does not

have to be perfect. You know, I don't think that's the standard regulators are looking for. But if you do not have a process, that makes it really hard to explain that, you know, this is a one-time mistake rather than a systemic issue that the company is facing.

Wayne Stacy 38:37
So, Ali, that leaves us at a great point that if you're reacting, there really doesn't seem to be any way to adequately manage any of these requests. So, this needs to be something at the beginning of your build out, not at the end.

Ali Jessani 38:55
That's exactly right. I mean, and you know, in privacy world, we often talk about privacy by design, incorporating privacy at the build stage, and now DSR [data subject rights] requests have to be a big part of that as well.

Wayne Stacy 39:10
Perfect, yeah. And I think when I listen to other presentations, people are talking about privacy by design, the old pieces of it, the cybersecurity pieces now with AI rolling that in, but you don't hear as much about this in the design phase, and I think this is a great, maybe warning to people that if you've got 30 days to fix this, it's probably too late if it's the first time you're hearing about it. So they need to reach out a little earlier to to folks to figure this out.

Ali Jessani 39:41
Yeah, and great point on the AI point. I didn't get a chance to talk about that, but that is, AI is just making all of this more complicated, right? Every company is gonna want to be an AI company. They want to train their AI models, and if you're using personal data, you have to think about how that intersects with your model. Like if someone makes a deletion request, and you're training your, you know, their data on your model- how do you exercise that deletion request, or are you taking the position that you weren't using their personal data, and so it's outside of the scope of the law altogether? I mean, these are complicated issues that companies are dealing with in real time.

Wayne Stacy 40:21
Well, I'm sure we'll get an opportunity to to talk about those more. I'm fascinated to hear about how you delete personal data that's already been ingested by an AI model. That is a computer science trick as well as a legal trick. So that'll be the next lecture. So thank you.

Ali Jessani 40:39
Yeah, thank you for having me. Really appreciate it.

Transcribed by Otter.ai, cleaned with the help of Claude, reviewed by BCLT staff

WILMERHALE

Data Subject Rights

Obligations, operational realities and regulatory expectations

Ali A. Jessani
Counsel, WilmerHale | Washington DC

SPEAKER

Ali A. Jessani

Ali A. Jessani
Counsel
Privacy & Cybersecurity
Washington DC

- Advises clients on privacy, cybersecurity and other regulatory risks related to data protection, with particular experience in US state privacy compliance, including the CPRA.
- Counsels on health privacy (HIPAA and state non-HIPAA health data laws), the FTC Act, state comprehensive privacy laws, financial privacy, employee data, targeted advertising and biometrics.
- Clients include healthcare organizations, data analytics providers, advertising agencies, social media platforms, financial institutions, B2B companies and start-ups.
- Guides companies through security incidents and regulatory investigations, and on data rights, integrity and governance issues raised by AI.

AGENDA

Five questions we will cover

01	What are data subject rights (DSRs) and what obligations do they create?
02	What laws govern DSRs?
03	What are the challenges and risks businesses face when operationalizing DSRs?
04	How do those obligations vary based on a business's specific context?
05	How are regulators addressing DSR compliance?

QUESTION 1

What are DSRs and what obligations do they create?

The rights

- Access / right to know what personal information is collected, used and disclosed
- Deletion of personal information, and correction of inaccurate information
- Portability — a copy in a usable, transferable format
- Opt out of “sale,” “sharing” and targeted advertising, and of certain profiling
- Limit the use and disclosure of sensitive personal information; appeal a denial

The obligations they create

- Provide and monitor designated intake channels, and verify the requester’s identity
- Meet short clocks: under the CCPA, confirm receipt within 10 business days and substantively respond within 45 days, extendable once by 45 days with notice
- Effectuate the request across systems — including instructing service providers, contractors and third parties
- Explain the outcome, including any denial based on an exemption
- Keep records of requests and responses for at least 24 months; California also requires formal training for staff handling requests

QUESTION 2

What laws govern DSRs?

The comprehensive state laws

- The CCPA, as amended by the CPRA, is the most detailed US regime and has a dedicated regulator in the CPPA
- 23 states have now enacted comprehensive privacy laws, each granting access, deletion and opt-out rights
- Most follow the Virginia/Connecticut model — opt-out for standard processing, opt-in for sensitive data, enforcement by the state Attorney General
- Applicability turns on revenue and processing-volume thresholds that differ from state to state

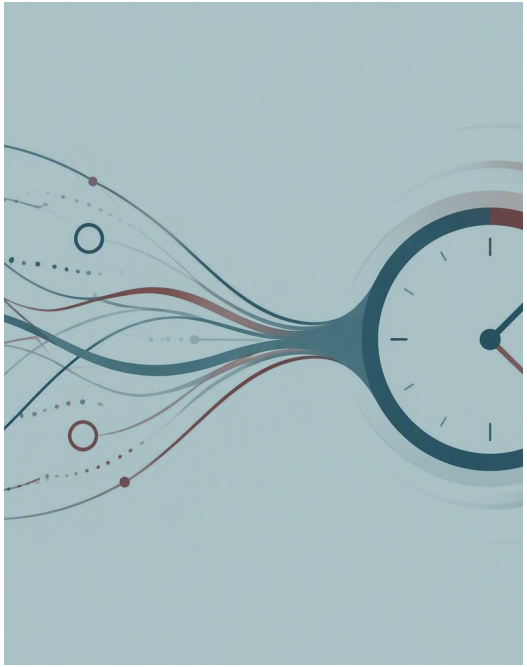
What sits alongside them

- Narrower consumer health and data laws in Washington, Nevada and Florida add further rights
- Data brokers have increased obligations in certain states (e.g., California and New Jersey)
- Sectoral regimes — HIPAA, GLBA and FCRA — can displace or carve out state law rights entirely
- The FTC Act reaches deceptive statements about how requests are handled
- There is still no single federal comprehensive privacy law, so the strictest state standard often becomes the operating default

QUESTION 3

Challenges and risks in operationalizing DSRs

- Fragmented intake — requests arrive by email, web form, chat and support channels and are not centrally logged
- New tools and laws are making it easier for consumers to submit requests
- Incomplete data mapping — personal information sits in systems the privacy team cannot see, including backups
- Identity verification — too little creates disclosure risk, too much collects data the business should not hold
- Vendors and downstream recipients — deletion and opt-out instructions must be passed on and evidenced
- Recordkeeping gaps — an inability to demonstrate compliance is itself a regulatory finding
- Opt-out interfaces that are asymmetric or friction-heavy invite dark-pattern allegations
- AI is making all of this more complicated



QUESTION 4

How obligations vary with a business's context

Your role in the transaction

- A controller or "business" owns the response; a processor or service provider must assist and follow instructions
- Contracts routinely impose commitments beyond the statutory baseline

Sector and data type

- HIPAA, clinical research under the Common Rule and financial privacy carve-outs can displace state law rights
- Sensitive data — health, biometric, precise location — carries added limits and consent requirements

Who the individual is

- California uniquely extends rights to employees and to individuals acting in a commercial or B2B capacity
- Most other states exclude commercial and employment context data from their rights regimes

Scale and jurisdiction

- D2C companies have more obligations than B2B companies
- Data brokers have the "most" obligations
- DROP requirements in California will meaningfully increase complexity

QUESTION 5

How regulators are addressing DSR compliance

$1.55M

Healthline Media settlement with California — the largest CCPA resolution at the time, involving unhonored opt-outs

$632.5K

CPPA penalty against Honda for asymmetric opt-out flows that made refusing tracking harder than accepting it

$1.35M

Tractor Supply settlement with California over notice, opt-out and third-party contract failures under the CCPA

- US enforcement has focused on DSR violations
- Cure periods are shrinking or sunsetting, so the first signal of a problem is increasingly an enforcement notice rather than a warning letter.
- DSR non-compliance is “low-hanging fruit” for regulators
- The common thread: regulators test whether a documented, demonstrable process exists.

CONCLUSION

Key takeaways

Rights are the visible part; the process is the obligation

Every regime asks the same thing — receive the request, verify the individual, act across your systems, explain the outcome and document all of it.

Timing matters

Response deadlines run from receipt, so escalation paths and decision templates need to exist before the first difficult request arrives.

As does context

Your role, sector, data types and the requester's status can expand or displace the baseline — map obligations to business lines, not to a single policy.

Regulators are paying attention

Enforcement turns on whether a documented, demonstrable process exists, and cure periods are shrinking.

Ali A. Jessani | Counsel, WilmerHale | ali.jessani@wilmerhale.com