Podcast Transcript

2022 DSIR Deeper Dive: Personal Data Deletion

Date: August 17, 2022

Guest: James Sherer and Nicole Sterling **Host:** Amy Kattman

Run Time: 23:00

For questions and comments contact:

James A. Sherer

Partner
New York
T: 212.589.4279 | jsherer@bakerlaw.com

Nicole L. Sterling

Associate
New York
T: 212.589.4282 | nsterling@bakerlaw.com

Kattman: Ransomware. MFA. Extortion. Fraudulent fund transfer schemes. These topics and many others make up the key findings section of the 8th Annual Data Security Incident Response Report, informally known as the DSIR Report. Each year, the incident response attorneys within the Digital Assets and Data Management Group, or DADM, provide statistics and analytics around the incidents they encountered the previous year in a report that is eagerly received by clients, vendors, media outlets and, frankly, anyone interested in or tasked with their company's digital asset and risks. I'm Amy Kattman, and you're listening to BakerHosts.

This, our eighth episode in the series exploring the 2022 DSIR Report, discusses why personal data deletion matters. Our guests today are James Sherer, a partner and co-leader of our Emerging Technology team and Nicole Sterling, an

associate in our Privacy, Governance and Technology Transactions team. Welcome to the show James and Nicole.

Sherer: Thanks so much for having us.

Sterling: It's great to be here.

Kattman: Nicole, what are some proactive steps businesses can take to improve their ability to meet the tight data breach deadlines now imposed in dozens of countries worldwide?

Sterling: Yeah. So, one thing that we have found lately with a lot of the companies that we deal with is that there are certain things you can do to speed up your reaction when you have a data breach. Certain things, of course, you can't deal with that you're dealing with as they come at you, but one of the things that we really wanted to get into the DSIR this year were these sort of five steps that we think people could be thinking about in advance to help speed things up. And one is just simply knowing which of the international laws and which regulatory authorities your company is under. Another has to do with recognizing the different types of personal data because personal data, the definition of personal data, can vary depending on the law that you're under and in particular sensitive personal data can vary. So for instance, under some laws, financial data is sensitive, other laws not so much. Another one is to understand your company's global business profile and their compliance posture, because companies have different risk tolerances and different ways that they are willing to take on certain risks or less risk depending on, for instance, have you been subject to a regulatory inquiry in a particular country.

Also, another one that gets missed all the time that we're waiting on when companies are tracking this down, is the information that we commonly need for notice forms. Things like the full company name and address in a particular location, or the business identification number or tax identification number. And then finally, we would recommend remembering to account for the time it takes to translate all the forms that you have to fill out or submit to regulators into whatever language or languages that you are going to need to be dealing with.

Sherer: To Nicole's points here, really, a lot of these steps speak specifically to good information hygiene. Understanding how the organization manages this information and just digging in deeper to what the actual practices are. Data security incident response, it is a challenging time period, because obviously you're responding to and dealing with an emergency. You often have some pretty truncated timelines to deal with, and unusually for the management of information, separate and apart from how the business does its day-to-day operations, the organization is speaking on behalf of itself as a whole, for how it manages information, and that is a very, very different discussion than it often has.

We've seen many, many clients deploy a kind of federated approach, which is essentially a delegation out of responsibilities related to the management of

information and saying here are some general principles we expect our business units to know best for what to do with their information. Go and do it. Execute on this. It is very, very difficult to centralize some of those decisions and to keep track of what is going on, which speaks to this importance of trying to figure out what is going on before you absolutely need to figure out what is going on. To un-ring that bell is impossible, but to go back and examine practices and say, okay, well, here is what we were doing. Now that we have to evidence exactly what happened, or to come up with a colorable story as to what we understand happened when we're responding to regulatory inquiries or when we have to send out information to our customers, to our employees, to other individuals who might have been affected.

Sterling: And I think sort of at its base, too, it is this issue of knowing who to ask to get the information you need within the company because a lot of times that becomes very difficult and we're waiting for things to work up chains or across chains, or back and forth across subsidiaries, and it just gets very confusing and we lose a lot of time as we're just trying to get sign-off on certain actions.

Sherer: In another consideration, within this knowing what is happening, recall, when a data security incident occurs, it is not the most calm time in the organization, and oftentimes certain IT assets that you might rely upon otherwise to figure out who does what and who is located where and how to contact them may not even be operable. We've had instances where clients have reached out to us to say hey, our database for our consumers went down. We've got a bunch of suppliers we need to contact. We no longer have access to their contact information. You worked on a data asset inventory. You've got a lot of this information on your systems or that is maintained in this third party. Can you help us get access to that so that we can go ahead and do the next steps of our process now, to respond to this incident?

So some of the issues that you'd think of as being just practical applications of this, require a different approach because of the nature of data security incident response.

Kattman: Let's dig deeper into over-retention of data. James, what are the benefits of proactively cleaning up the personal data your business holds?

Sherer: So, it’s, in some ways, the opposite of what information you need at hand during a data security incident. This is, practically speaking, good hygiene for the way in which you manage information, and the data security individuals, I've heard it stated as this surface area issue, the less information you maintain, and certainly the less personal information you maintain, the less an attacker has to attack. The less places it is kept, a smaller or more succinct, more focused picture of individuals’ data that an organization maintains helps it to focus better on what it is protecting. The more you know, the better off you're going to be.

It also can help with business operations. It is not just about regulation. When you're maintaining information, you want to make the best decisions you can, and the best decisions are predicated on the best sets of information. So if you've got

smaller pictures of data, it is also more likely that that is the correct data. Carrying on information about individuals over time can lead to outdated data sets. It can lead to poor decision making and surprises to consumers who might say why are you still maintaining information that is a decade old. We've had clients going back to the 1970s lately to say, hey, we still have this information. Should we have it? And it is often kind of the response that you'd get. If you're asking the question, in some ways you've already answered the question. If you can't think of a good reason to have it, and you're just trying to find an excuse, then it is likely not the best course of action forward.

Sterling: I think a lot of times, too, we end up talking to companies as a data breach unfolds and there is information or data in that set of data that is coming back to them that they're saying why on Earth do we even have this. Why are we holding onto this? Or even, I thought we got rid of this already. So, there are pieces around that that, you know, there is a lot of surprises, I guess, that come out of dealing with data breaches.

Sherer: And when you're not in the midst of a data security incident response, when you're not in the middle of a breach, you can be a little bit more sophisticated about approach. You can certainly be more strategic. And to Nicole's point, yes, we've both been part of response teams where it is a journey of discovery, and I will say this, Nicole and I, wonderful at examining your information, but probably not the people you want to examine your information in the first instance. It is a hurried process. At that point in time there is not a lot of opportunity for course correction. There have been plenty of instances where there is a data security incident. You're digging into databases, you're evaluating information stores, and you're finding these surprises about operational issues.

For example, oh, it turns out that our systems allow us to capture the information of minors. That is a surprise. It turns out that we've collected a lot of information about minors, or at least the system that we're using seems to indicate that that is the case. Now, normally if you would, you discovered this outside of a regulatory response requirement, you'd be able to examine it further and say, is this truly the case. Can we examine this? Can we solve for this right now and improve our business processes and delete all this information? However, if you're in the throes of a business compromise, the parameters are very, very different and the responses require different sorts of evaluation as well.

Kattman: What are some of the laws, both international and domestic, that call for limiting personal data storage, James?

Sherer: So, the concept of the law here is pretty wide and it can come from some pretty varied circumstances. I think when we look at the most direct application and what we've got a little bit of history with would be that GDPR out of Europe, which requires organizations that are governed by the GDPR to limit the information that they collect, certainly, and to do it purposefully and then to delete information they're not using. So, speaking about that limited data footprint and being very, very cognizant of it, and intentional in applying data limitation, the GDPR is and has some direct application to that. We're also seeing the advent now of the

CPRA in California. The CPRA has some brand new requirements that are going to go into effect January 1, 2023 and be enforced as of July 1, 2023. Here, there is a requirement for organizations to explain, present and disclose what types of personal information and sensitive personal information, a couple different categories of information with a lot of granularity, out, to disclose information out to California residents, and by extension a lot of other individuals in the U.S. and abroad. These are brand new requirements and, by extension, they end up essentially informing organizations about how they should be managing information.

So, you think about it, like what kind of picture are you presenting that seems accurate. What seems realistic, especially to a consumer whose information you might maintain? We also have some additional pressures from organizations like the FTC and say, well, what disclosures have you made to individuals when capturing some of that information, and how closely are your practices aligned with those representations. If they're not aligned, if they don't match up, if something happens, or if there is an inquiry and there are some challenges between those representations and actual practice, then there may be the possibility of enforcement actions. We've even seen some lately related to information governance, again both in Europe and in the United States, which speak to challenges with over-retention of information, then some kind of compromise, or even just indications of use that the regulators have become very interested in.

Sterling: And I think James's point, too, about having to deal with whatever policies you put in place yourself, both from a retention policy and a retention schedule, piece is really important as well, because a lot of companies and we have them come to us and say things like we have this retention policy. We have this retention schedule they were created maybe four or five years ago. We're not sure anything has happened with them since. What should we be doing with that? And I think that is a question we get asked a lot. I know it is a question that James deals with a lot, so I'll let him jump in and discuss that if he wants.

Sherer: So, the retention schedule should be evidence of both what an organization is doing and the guidance it is giving to the individuals within the organization who are responsible for maintaining that information. For a very long time, the record retention schedule, with few exceptions, speaks to how long an organization must maintain that information. What should they have available? What are they required to have in their files, whether in paper or electronic form mostly now, if they were asked to respond to a regulatory inquiry associated with that information? What we're seeing now is the capping or the end, the collaring of that type of responsibility, where it is not just make sure you have this type of information for this period of time, but also don't maintain this type of information for longer than this period of time. Certainly don't maintain it longer than absolutely necessary, and understand that if you are maintaining this information, you have certain requirements about the way in which you are maintaining it. How are you protecting it? How are you using it? If you're saying you're only using it for some very specific purpose, let's say for fraud detection or incident prevention or for legal process or legal hold issues, well, you can't go along and

market to that information if you're keeping it for a different purpose. So, purpose limitations and restrictions, many of which are then further supported by getting rid of information and good data hygiene.

Sterling: And this idea of necessity is one that is built into a lot of the data protection and privacy laws that we see. This idea that you can have personal data for as long as you need it for the purpose for which it was collected, or sometimes for a related purpose. Where companies I think get into trouble with that or have trouble understanding when they should get rid of that data has to do with what is necessity and is it necessary because the marketing department wants to collect a bunch of data and do analytics and figure out how to market the business better or is it actually only necessary, for instance, in the context of the transaction for which you originally got that data.

Kattman: Nicole, can you discuss what types of regulatory action businesses can expect for noncompliance and how they can prevent it in the future?

Sterling: Yeah. So, one of the things that we are actually seeing regulatory action around in the breach context, but generally, as well, is around over-retention of data. We see some regulatory action related to not complying with what you say you're going to comply with within your own policies. So, for instance, if you put it out there in your privacy policy that you keep data only for as long as it is necessary and maybe even attach a timeframe to that, like, two years or four years, and then you have a data breach and suddenly all of this data they realize has been in your systems for six years. So, we have seen enforcement action around that piece.

We've seen enforcement actions around keeping data longer than regulatory authorities think that you need to be able to keep it. Just in the last couple of weeks, we've seen a couple of enforcement actions that have been somewhat interesting, I think, out of the European Union. One comes from Denmark, which, actually the Danish Data Protection Authority has been somewhat active in the space of retention recently, but they had this decision few weeks back that looked at an entity and its retention of data, and realized that they could actually order the entity to create a data map, which they did, and then on top of that, put in obligations around retention. So, that piece I think was interesting because we haven't seen data maps really addressed a whole lot as part of the enforcement action piece around these retention and deletion requirements.

Another one out of France recently looked at geolocation data specifically and found that it was being excessively retained in relation to rental car use and that they felt that these, that rental car drivers essentially did not need to have that data retained for longer than, sort of, the immediate rental period to be able to determine, you know, where the car was used. And this was over the, sort of, company’s idea that the data needed to be retained to help them understand, for instance, the car maintenance schedule and things like this. But the French Data Protection Authority said no, they needed to get rid of the data and ordered deletion. And we have seen a number of enforcement actions go toward that

piece of ordering the deletion of data that a regulatory authority feels has been overly retained.

Kattman: James, do you have anything additional you'd like to add?

Sherer: In 2021, we actually saw some enforcement related to specific requirements for data retention. Now, this is still about retaining information that should have been managed, and it was more about the form in which that information was managed, but it was a matter that we all paid really close attention to in the information governance world. It was a combination of a very, very high set of fines that totaled $200 million when applied to the organization and the manner in which the information was managed, which in this case was on some texting platforms, including WhatsApp.

So there, there were requirements for maintaining that information in a certain way. I think it was the WORM format, write once read many, speaking specifically to broker-dealers. We saw the fine. We saw the notifications. We thought that was it. And very, very recently, there were a slew of other similarly situated organizations that started to put their own reserves in place to deal with what they expected those fines to look like for their practices. And one of the challenges here was what the clients were doing was entirely expected, given what had happened during the pandemic, when everyone went home, everyone was using different communication platforms to continue to communicate to get business done. Getting business done was the important part. The world may have been ending. There were different circumstances at play and now, in some ways, the bill seems to be coming back to get paid. We don't know and a lot of organizations don't know exactly what all of their individual constituents are doing and what they've been doing for the past couple years.

I believe that regulatory action will really speed up if we start uncovering a lot of additional challenges that were simply not on the radar of organizations that were just desperately trying to get to the next day and the next day, and possibly the next week during the course of the last couple of years. So, digging in and examining some of those hygiene issues, certainly it starts with a strategy, but when thinking about regulatory enforcement, it is also how you articulate the story of what happened, because at the end of the day, you know we talk about these regulators as though they're up on the hill and it is only top down and in some ways monolithic in approach, and it is truly not. Regulators are people. They're trying to interpret the statutes. They're looking, I believe this in my heart, looking in the first instance at protecting consumers, protecting individuals, protecting their personal information.

What is the story back to them to explain why a given client, a given organization, has really tried to embed and incorporate those practices into the work that they've done? Those are the types of things I think that we’re really intent on explaining to regulators in response to their, these increases or potential increases in regulatory enforcement as we move forward.

Sterling: And I think we see a lot of regulators looking at reasonableness as a sort of standard for retention, generally. Like, is it reasonable that you've maintained data for a particular time period. We've seen that even in the U.S. with a couple of recent enforcement actions under the New York Shield Act, this concept of reasonableness. But we are seeing more and more regulators go toward this idea of either ordering companies to develop retention schedules to comply with the retention schedules that they have developed or to have a better understanding of the data that they have, and also to delete data. It has been interesting to see a number of actions, lately, coming to this point of data deletion and ordering certain types of data to be deleted, and we're seeing that, I think, both in the retention space, but also with other types of data that companies might hold, specifically around certain types of AI uses. We've seen regulators order that data be destroyed, and also around sensitive data and other types of data that they just feel is not reasonably necessary to the business.

Kattman: Thanks so much, James and Nicole, for this valuable information.

Sterling: Thank you.

Sherer: Yes, thanks so much.

Kattman: If you have any questions for James and Nicole, their contact information is in the show notes. As always, thanks for listening to BakerHosts.