Podcast Transcript

2023 DSIR Deeper Dive: How International and Domestic Regulatory Enforcement Spotlights the Information Governance Tensions Between ‘There’ and ‘Here’ and Between ‘Keep’ and ‘Delete’

Date: November 21, 2023

Guest: James Sherer, Brittany Yantis, Luke Record, **Host:** Amy Kattman

Run Time: 14:33

For questions and comments contact:

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

Brittany Yantis
Associate
Washington D.C.
T: 202.861.1525 | byantis@bakerlaw.com

Luke Record
Associate
New York
T: 212.847.7045 | lrecord@bakerlaw.com

Kattman: Managing digital assets requires the efforts of the whole enterprise. The 2023 issue of the Data Security Incident Response report, or the DSIR, includes more content than ever regarding the data ecosystem and how companies can best manage their digital assets as they move through the life cycle of data.

The DSIR, of course, dives deep into the annual incident response trends and analytics our clients and friends depend on. It also covers topics such as global privacy, ad tech, the increase in litigation, healthcare privacy and compliance, and the latest in emerging technology. I am Amy Kattman, and you are listening to BakerHosts.

We are back with a Deeper Dive series covering key topics in this year's DSIR. On today's episode, we discuss the information governance tensions with international and domestic regulatory enforcement. Our guests are James Scherer, Partner and Co-Leader of the Emerging Technology team; Brittany Yantis, Associate in the Digital Assets and Data Management Group; and Luke Record, Associate in Litigation. Welcome to the show: James, Brittany, and Luke.

Sherer: Thanks so much.

Yantis: Thanks for having us.

Record: Happy to be here.

Kattman: James, let us begin with you. Would you tell us about the current regulatory laws in Europe and those here in the United States? And are there parallels between the two?

Sherer: Absolutely. So, when we are talking about records, I think there is three main parts here, two being the international components. The first is this idea that you've got regulations out there that speak to how long organizations should be expected to have certain types of information available, so if a regulator comes back and says, hey, do we have records of this type of behavior or these events, the organization can hand over those records in response. That has been the traditional practice where you just want to make sure you have the available information if you get that type of inquiry, and then that extends to regulatory, or investigative purposes, or litigation. However, data privacy has somewhat turned that on its head, started with the GDPR, that General Data Protection Regulation in Europe and the Storage Limitation Principle, which said you can only keep Personal Information long enough to satisfy the purpose for which you collected it. So, you can't just keep it forever, whereas that was some of the older types of practices that we saw within organizations.

Now that sensibility has since traveled over to the United States, and we've seen it in some shape or form within the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and there under 1798.100 of the regulations, says that you have to disclose how long you keep the information and/or why you are keeping that information and specifically personal information and sensitive personal information.

So, through these two different privacy types and privacy-oriented regulations, now we have a pressure to look at what the retention periods are and why you're doing it, and this is brand new. So, the parallels are there, and I believe that the parallels exist in part because information travels across borders. It does not

respect in the same way the borders of a specific country or in Europe's case, the entire continent and those organizations that are, are working within that area.

So, we do have some new requirements for the way in which you maintain that information on behalf of an organization, but also what the notice requirements are too. So, laws and regulations oriented toward giving people more information about the way in which this information is maintained, it is to give people, individuals, more agency, and a better and clearer look into organizations practices or how those organizations maintain information about individuals. It is easy and sometimes very, very low cost to copy information. Now a lot of these laws are oriented toward better management and better information to people about the information the organizations maintain.

Kattman: Thanks, James. Brittany, how do recent European enforcement actions play a role in what regulatory bodies do domestically in the U.S.?

Yantis: I think it is going to play a pretty large role. So far, we don't really have a lot of enforcement in the U.S. for all these new privacy laws, and new ones are getting passed every month it seems like now. So, I think it is only natural that the U.S. regulatory bodies are going to look to Europe and the similar requirements in the GDPR to determine how to enforce here in the U.S.

So, to give you a sense of those actions there have been numerous actions recently related to information governance and retention under the GDPR, and those fines definitely are not nothing. And so, it's something to consider and understand. Recently, the Hungarian Supervisory Authority imposed a fine of approximately €248,000 on an internet and broadcasting service provider for the creation and lack of immediate deletion of a database test.

The French CNIL imposed a €600,000 fine against an electric utility in France for, among other issues, retention compliance problems. The French CNIL again imposed an €800,000 fine against a French company for retention appliance problems. Italy, as well, their supervisory authority imposed a two million fine on a social media network, in part for retention compliance issues. The UK Supervisory Authorities Information Commissioner's Office imposed a fine of over €7.5 million on a facial recognition company for, among other issues, lack of clear data retention policy documentation and I think that kind of goes along with the rise of AI and these newer issues. And I think data retention is certainly going to be an issue that these regulatory authorities are looking to when it comes to newer technologies, like AI, and the risks that those pose. So certainly, fines they're definitely high and they're not nothing, and so, I think it's a good kind of road map to see where enforcement is going over in Europe and how it will play out here in the U.S.

Kattman: Thanks, Brittany. Luke, can you tell us what is the Safeguards Rule, and how it impacts organizations?

Record: Sure. So, the Safeguards Rule was promulgated under the Gramm-Leach-Bliley Act, often known as the GLBA. And under 16 Code of Federal Regulations Part 314, it applies to financial institutions that are not otherwise subject to a federal functional regulator. So, we're talking about firms like financial advisors, accountants, tax preparation firms, and even retailers that issue their own credit cards. So, some people have this notion that the Gramm–Leach–Bliley Act, and in turn the Safeguards Rule, only applies to certain things and financial institutions that we traditionally think of. But this Safeguards Rule is applicable in a much broader sense, so that is something really important to keep in mind.

And the rule prescribed a number of different practices aimed towards achieving information security, confidentiality and integrity, as the name suggests, it's intended to safeguard customer information. But for purposes of our discussion today, the provision we're really interested in is the data retention provision. Which says that an organization, again a financial institution as defined under this rule, is not allowed to keep customer information for longer than two years after the last date the customer information was used to provide products or services. Now there are a number of exemptions, such as if that information continues to serve a legitimate business purpose, or the deletion of such information is not feasible due to the manner in which it's maintained.

But I do think the Federal Trade Commission, which promulgated the rule, intends for organizations to comply and so, as Brittany was saying, across the pond they really are trying to enforce these data minimization provisions under the GDPR. Similarly, here, both under state data privacy laws but also under the federal regulation which we are discussing now, there is this incentive to delete information when it no longer serves the purpose for which it was intended for such as providing services to the customers. So, it'll be very interesting to see the ways in which these exemptions are taken advantage of, or whether organizations are really going to try to strictly adhere to this two-year requirement.

Kattman: James, what tensions do you recognize between keeping and deleting data?

Sherer: The first tension truly is past practices of organizations. It's been easier now with the advent of a lot of electronic systems to maintain information indefinitely. 50 years ago, it was easier to see how important data management practices were when you collected paper and you had warehouses and storage areas full of them. There was a tangibility to that information, and you had requisite experts who were moving paper around, and had to make sure that they had access to records. And you could lose things if you had too much information, it was unavailable. I mean that changed with the advent of cheaper storage and systems that made it very, very easy to create documentation, instead of sending an idea to the secretarial pool to have a memo drafted up or to document something, and instead people will generate a lot of information.

That is run full speed now into concerns we have about personal information and what we've seen reflected in the data privacy rules. So that tension between the ease of creating and maintaining information, sometimes indefinitely, running full-

bore into data privacy law and expectations now that information is deleted if you don't need it, means that there have been years and years, and sometimes decades, of periods of time where information has just built up, and now organizations are seeing the challenge of trying to address this, and sometimes all at once in trying to work according to the law.

Kattman: I have one more question. Luke, could you talk about how organizations can move forward efficiently and practice good information governance habits?

Record: Yeah. So, it's critical from the onset to develop clear policies surrounding the handling of records and other sorts of information. And so, we typically advise drafting what is called a records and information management policy which lays out the various roles and responsibilities for different stakeholders in the organization, and the ways in which employees will be held accountable, and where they can go to resolve questions concerning the handling of information.

And in addition to the policy, there should be a records retention schedule which provides a more granular accounting for all the different records and prescribes a retention period. So, there you have in one place, and every employee should have access to this policy and accompanying schedule, and know the expectations surrounding how long we are to keep this information. And again, the lines of communication, the channels of communication, should always be open and it's critical that everyone is on the same page.

And in addition to employees reviewing this and acknowledging it, the IT department should be heavily involved and where possible, the technology available should be leveraged to allow for the more effective implementation. Now of course it's not always so easy as just turning the policy and the schedule into practice. There are often some bumps in the road.

Kattman: Brittany, do you have anything to add?

Yantis: Yeah, and just to add on to what Luke said, I think you can put these policies in place, get them drafted and really create a robust information governance program at the policy level, but then you really have to put in the work to figure out what is really going on within your organization, where is the data being kept? What are people actually doing?

So, you have to put in that inventory work, talk to various stakeholders, like the IT department, legal, just various business units to find out where they're keeping their data, how they delete it, and where all that information is, and really getting on the ground and find out what's going on so you can really achieve what the art of the possible is, after you put those policies in place.

Kattman: James, Brittany, and Luke, thanks so much for joining us today.

Sherer: Thanks so much for the opportunity.

Yantis: Thanks so much.

Record: Thanks for having us.

Kattman: If you have any questions for James, Brittany, or Luke, their contact information is in the show notes. As always, thanks for listening to BakerHosts. Comments heard on BakerHosts are for informational purposes and should not be construed as legal advice regarding any specific facts or circumstances. Listeners should not act upon the information provided on BakerHosts without first consulting with a lawyer directly. The opinions expressed on BakerHosts are those of participants appearing on the program and do not necessarily reflect those of the firm. For more information about our practices and experience, please visit bakerlaw.com.