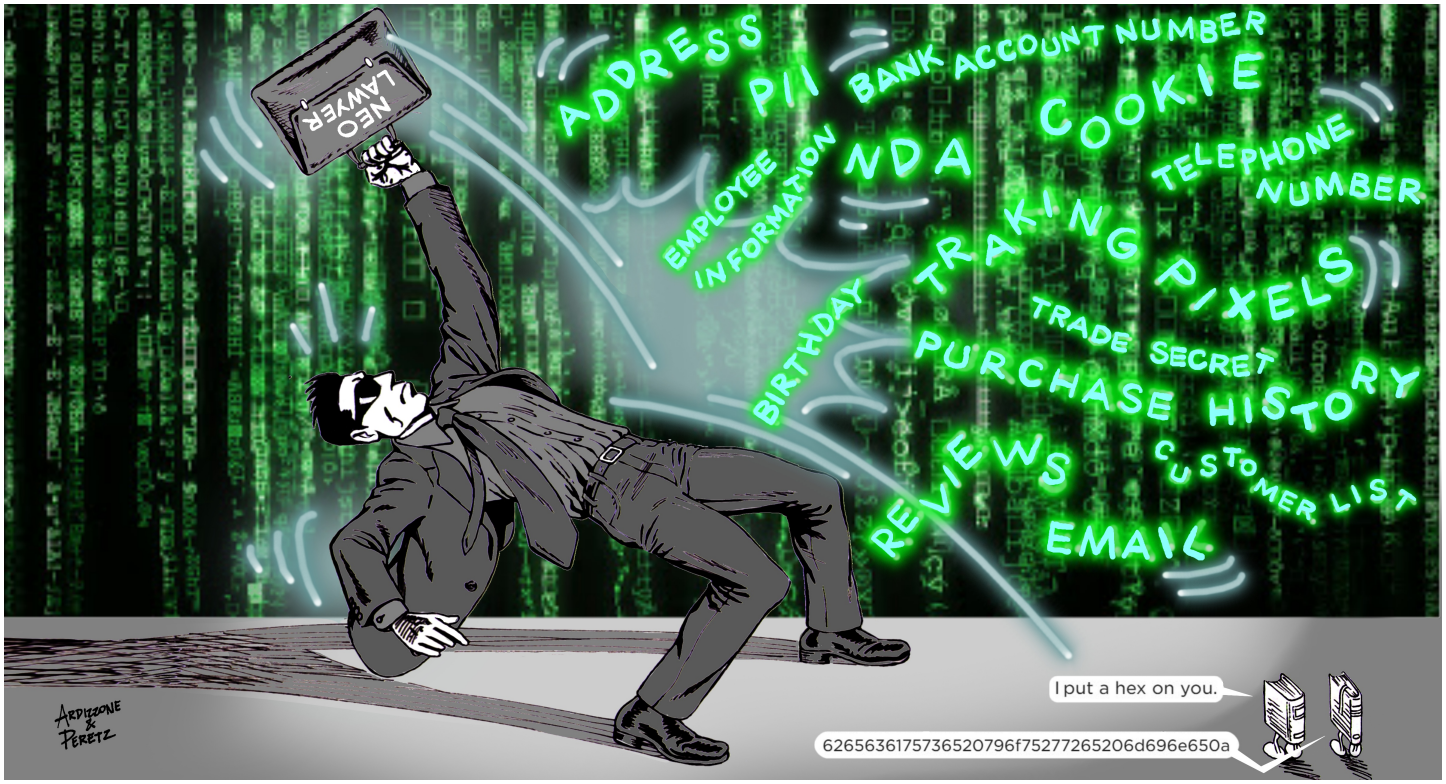


The Operational GC: Dodging the Data Bullet

Information Governance





There are more data-related laws than you think

There are two potential starting points to get your organization's data under control: mapping all the data you have and understanding requirements related to it. From your colleagues' vantagepoint, "requirements" are synonymous with the law, so they expect you to identify the relevant regulations and map those for your company.

Remember that data-focused laws are not limited to those with non-disclosure provisions. Depending on your industry, there may be important laws specifying data retention requirements. For example, if you extend consumer credit, the Equal Credit Opportunity Act requires lenders to maintain data related to underwriting decisions for at least 25 months after the data is used to test for potential disparate impact. If you work for a public company in the United States, the SEC dictates that your organization save audit-related documents and communications for a minimum of seven years.

Consider the states where your business operates as well. Federal privacy laws, such as the Gramm-Leach-Bliley Act, often do not preempt state laws related to privacy and data retention. For example, the lifespan of medical records is left to the discretion of each state.

Manage your data where it lives, don't copy it

Copying your data so the legal department can search it or to respond to one-time legal events should be avoided at all costs. Copying your data introduces avoidable risks and version control complexities for enterprise data management, as well as challenges enforcing access controls and compliance with data retention and disposition policies.

Rather than duplicating data for the law department, focus on data governance tools and methods that bring the IT and legal teams together. These tools and methods allow organizations to connect multiple viewers to a unified data source, while tracking access and potential data changes. Managing your data where it ordinarily lives keeps it safe behind your firewall and ready for immediate and proper data mapping, discovery, and action.

Don't forget the data under the floorboards

It's not enough to manage the newest data repositories garnering work-from-home headlines (e.g., Microsoft Teams, Slack, and Zoom). Those represent the tip of the iceberg when it comes to truly assessing your enterprise data footprint and risks.

For the most part, enterprise data and risks lies underneath the applications that power your company in the infrastructure layer, where all of this data finally lands and has been landing for years.

Names like Isilon, NetApp, VMAX, VNX, HDS, and Data Domain may not ring a bell to you, but they will to your IT teams. This is where the vast majority of your corporate data has been accumulating for decades. Typically, the application designed to provide functionality to your business handles data in a transitory fashion, calling it and using it when needed, and then passing it back to the infrastructure of your IT system.

Plan to partner with your IT team to access this data to pipe it into your data governance process. Look to your software vendors for metadata about how this data is formatted and saved.

Sell the value, not the stick

Giving your colleagues a long list of places to look for data and information to categorize does not typically generate enthusiasm. Focus your message on the benefits of marshaling, sorting, and controlling access to your corporate data. Remember that benefits are not a one-size-fits all proposition: they vary by department.

Your sales team may be hoovering up customer and prospect data at a torrid pace to prioritize leads, target the right decision makers and influencers, and memorialize customer touch points. Depending on the incentive scheme for the sales team, some team members may be overly protective of the data they have assembled, fearing that others in the company might take their leads or somehow outshine them.

Another challenge of working with salespeople is their focus. Salespeople have laser-like attention on hitting their quota. Administrative tasks slip to the bottom of the To Do list and become overridden by their sales goals. And it's hard to argue against the importance of sales.

Fortunately, corralling all your company's data, particularly unstructured data from contracts and information from systems in other departments, can turbocharge their sales efforts. Explaining that well-organized data governance can create new slam dunk sales opportunities will grab their attention.

How does data governance generate new sales?

A key trend in business-to-business selling is called Account Based Marketing (ABM), where marketing and outreach efforts are targeted at specific people and touch points at target accounts. ABM is based on information about accounts, all which can be aggregated across your entire organization with proper data governance. For example, you might find out that your procurement team has a relationship with the company that your salespeople are targeting. Getting everyone together to build an information inventory will empower you to find those hidden relationships that can drive new sales.

Once you get into more sophisticated business-to-business sales, strong data governance is essential to getting sales closed faster. It's not uncommon for large clients to require representations that your company is ready to comply with a growing tangle of privacy laws. Your company is not going to be able to safely make those assurances until it has all of its internal data under control. Tell your salespeople that this process of information gathering, classification, and management will remove blockers in the sales process. They will be much more supportive of your efforts.

Use different strategies for different teams

Outside of sales, other teams in your company will also have vested interests that dovetail with better data governance. For example, your ops team and customer success team will want to track all manner of customer interactions to get a full picture of client engagement and rapidly spot emerging issues. Building a data governance program enables you to centralize this information across your organization, which is essential to providing this 360-degree view of the client.

Use pivotal events as a catalyst to get caught up

When your company is going through a major audit, financing, or transaction, you are going to receive numerous due diligence requests that cut across the organization. For example, you might be asked to describe every relationship where there is an exclusivity. To do so, you may need to go through all the contracts held by procurement, sales, partnerships, and operations. Or, you may have to develop an inventory of all the personally identifiable information your organization collects.

You can use these pinnacle events as an opportunity to build the foundation for your ongoing data

governance activities. By the time you finish gathering all the information, your colleagues will begin to appreciate how much easier it would have been to keep track of that information on a day-to-day basis rather than scramble for it after the fact. Leverage the memory of the crucible of deal-closing as inspiration to implement new data tracking systems and processes before the next transactional storm hits.

Scavenger hunts for data, especially around events that are important to your entire organization also present an unparalleled opportunity for building relationships. Everyone in your company should be motivated to pull in the same direction and be more motivated to cooperate. Use this as an opportunity to map the processes in their department, spot future data issues emerging, and identify the key team members who will give you insights and access in the future.

Understand your contractual obligations

Sophisticated counterparties understand that they can be held liable for the actions of their suppliers and partners. They manage this by assigning data governance responsibilities to your company. You need to look beyond specific laws into your business agreements to fully map your data responsibilities.

Many organizations have contracts that require deletion of confidential information when the agreement ends. Which of your agreements have that term, and what confidential data is in scope for that particular relationship? If you do not have these answers ready, and a process in place to execute them, breaking up is going to be hard to do. Likewise, you need to know when a counterparty needs to certify that it has destroyed or returned your confidential data when the contract so requires.

State laws often require client notification when a data breach occurs, but the time frames for these may be longer than your contracts allow. As soon as a breach is suspected, you need to quickly identify whose information was impacted and when the contract requires you to tell them.

Don’t forget data about data

Countless data breaches and exploits have been tied to corporate insiders or a hacker gaining control of an insider’s credentials. Tightly controlling and auditing data access allows your team to quickly pinpoint leaks and abnormal behavior that could be the first clue about data leakage.

One of the circumstances where hearsay is admissible is when it demonstrates its effect on the hearer as opposed to the truth of the hearsay itself. Like this, even if there are inaccuracies in your data, it’s not uncommon for a tribunal or counterparty to inquire about who knew the data and when they knew it. Data access audit mechanisms enable you to answer with confidence when a particular person did or did not review certain information.

How to get started: indexing guidelines

Before you dig into piles of data and deputize each corporate department through your data roundup, create shared guidelines for how data should be categorized and grouped during the first pass. Within each data category, you may develop additional subclassifications over time, but there are questions important to note for all data at the outset of an audit:

- Is the data a temporary or permanent record?
- What format is the data?
- Are deletion rules determined by date created or date last accessed?
- What laws is the data subject to?
- Will the data be subject to discovery in the event of litigation?
- Do you have contractual obligations related to the data?
- Are there data breach notification requirements tied to the data?
- Who can access the data and can that access be tracked?
- Where is the data backed up?

Share the journey

In-house counsel across industries are going through similar processes in their own organizations. ACC presents multiple opportunities, such as the Information Governance Network to get feedback from peers about how to organize particular data and what are the best practices for controlling access to it.

Neil Peretz



General Counsel

Sawa Credit Inc.

Neil Peretz has served as general counsel of multiple companies, particularly in the financial services and technology industries, as well as a corporate CEO, CFO, and COO.

Outside of the corporate sphere, he co-founded the Office of Enforcement of the Consumer Financial Protection Bureau and practiced law with the US Department of Justice and the Securities and Exchange Commission. Peretz holds a JD from the University of California, Los Angeles (UCLA) School of Law, an LLM (master of laws) from Katholieke Universiteit Leuven (where he was a Fulbright Scholar), bachelor's and master's degrees from Tufts University, and has been ABD at the George Mason University School of Public Policy.

He previously co-founded legal technology company Contract Wrangler, which applied artificial intelligence to read legal agreements. Follow him online at linkedin.com/in/neilperetz.

John Sanchez



Head of Legal Technology

Congruity360

John Sanchez is Head of Legal Technology at Congruity360, a data governance software and services company with experience supporting customers in over 100 countries. He is recognized as an early pioneer in legal process outsourcing. He has served in executive leadership roles at both private and public companies, and more recently leading product and sales teams for legal and compliance software solutions. Sanchez holds a JD from UC Hastings College of the Law and a BA from UCLA. Outside of law, he is active with community and nonprofit organizations.