COSMOS
Navigate the Compliance Universe

CEP Magazine - April 2023

Randolph Kahn (rkahn@kahnconsultinginc.com) is Founder & President of Kahn Consulting in Highland Park, Illinois, USA.

Jay Cohen (jcohen@ghclaw.com) is Of Counsel to the law firm of Giordano Halleran & Cielsa and a Senior Advisor at Compliance Systems Legal Group in Wilton, Connecticut, USA.

Data and compliance: A guide to being an information herder, Part 2

By Randolph Kahn, Esq., and Jay Cohen

This is the second article in our two-part series: "Data and compliance: A guide to being an information herder." Part 1 of the article, published in the January 2023 issue of *CEP*, described the dangers of information hoarding, including the legal, compliance, and business issues affecting companies lacking adequate insights about the information assets they possess and how that information is being used, managed, protected, and retained.[1]

This installment provides practical steps and a high-level roadmap to help fix the sprawl of your company's information footprint so you can transform from a collection of information hoarders to an organization of information herders. We have divided this second installment into two parts:

1. General advice on developing a business profile assessment (BPA) that will enable you to better manage data and compliance.
2. Tips to address some of the specific data management issues and concerns highlighted in Part 1.

How to find and end information hoarding: The BPA

As we explained in Part 1, you cannot transform from information hoarding to information herding without understanding what information your company has, what obligations exist with that information, how long the information needs to be retained for legal or business reasons, and who should have access to it. Answering these questions requires a foundational understanding of what you are doing today as a business. Invariably, when we help businesses with data and compliance, we learn that management generally understands what business activities the company is engaged in but does not comprehend all initiatives, relationships, contracts, projects, and potential sources of revenue and risks across their enterprise and how this affects their information ecosystem.

Ask early and often, and be circumspect of easy answers

Companies often think they are doing one thing when they may be engaging in a range of other activities that are not readily apparent. When asking a business unit lawyer, "Do you know if anyone in the business unit is selling data to any third party?" the answer inevitably is incomplete or wrong because information selling or sharing is much more complicated and likely today; the laws addressing these activities are far broader. For example, under the definition section of the California Privacy Rights Act (CPRA), "'Sell,' 'selling,' 'sale,' or 'sold,' means

selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for monetary or other valuable consideration."[2] Privacy and security laws cover a wider universe of activities than many organizations recognize.

One insurance company executive who "painstakingly" described for us his firm's lines of business neglected to include its ownership of a commercial water company that implicated a new set of laws and regulations, including data governance and record retention requirements. This executive further failed to mention that, while the company had divested its banking operations, it still processed mortgages in a separate business unit. Finally, the client left out the company aircraft, which was subject to various federal aviation regulations, and its operations in many jurisdictions. None of this was included in the legal team's evaluation of data and compliance, even as information relating to all of these ancillary businesses was being hoarded—out of the reach of retention schedules and other compliance tools.

This is the reality for most companies, whether they know it or not. The way to address this void in understanding both their businesses and the applicable rules is through an in-depth BPA, which will form the basis of a deeper understanding of the company's business activities, the jurisdictions in which it does business, and the laws and regulations that apply.

Developing your BPA

You (and your team) need to methodically assess the major business initiatives, lines of business, and places in which business is happening and then document the findings in a usable format offering transparency to the organization.

With this baseline understanding, you then must go substantially deeper to understand how this business is being done, who it is being done with, what information is generated as part of it, and any associated data compliance requirements and risks. An energy client had applied smart devices to its transmission system and grid, as well as to millions of homes, in order to enhance energy efficiency and provide new insights into threats to its service. This raised complicated and open questions about who manufactured the smart devices, what information was being captured by the devices, where that information was sent, and who had a legal right to access that information. The company now knows who is doing laundry at 3 a.m. and who runs an air conditioner at very low temperatures. Smart meters and other controls can make the company run more efficiently and effectively; however, that information is now both a new potential revenue stream and an added source of risk.

Address your known business activities, but do not stop there

To look at this in another way, making a medical device is an obvious business activity for a medical device manufacturer; it is core to what it does for a living. The company's legal and compliance teams will consider laws and regulations related to the design, quality testing, manufacturing, marketing, warranty, service, and selling of the device. The BPA must capture the not-so-obvious to determine, among other things, what data is being captured, created, stored, or sold related to the medical device, including "personal" biometric data involving patients/consumers using the devices. Harvesting and monetizing the value of data are happening in most businesses; these activities need to be understood and "regulated" internally before they are regulated externally with potentially disastrous legal, business, and reputational consequences.

Going deeper into this example

- Does the medical device collect data—including specific categories like personal information, protected

health information, and biometric data? The laws and regulations regarding the use of such information will vary depending on the jurisdiction.

- Are third parties involved in the business activities? Third parties can assist in marketing activities, collecting payments, or be a company like Amazon Web Services that merely stores the data.
- What are the planned uses for the data collected or transmitted from the device? Will it be shared, sold, or bartered? Do any third parties have access to it?
- What data is stored on the device? Is the device ever returned to the organization or a third party for repair or service or at end of life?
- Is any data from the device stored in a data lake or warehouse? Is it aggregated with other business information? Is it sold, shared, or rented as aggregated data?
- How long is any data on this device being retained? For businesses with a European presence, is retention evaluated the retention based on the European Union's General Data Protection Regulation?
- Is support provided through a chatbot or artificial intelligence (AI) or with a connection to a mobile device?
- Are doctors allowed to connect to the device? What information is provided to an authorized medical professional?
- Does data from the device go to an iOS or Android app?

These are the kinds of questions you should ask related to any significant business activity at your company as you build your BPA. While this appears to be a complicated and lengthy process, the answers to these questions can be found in our organization and are essential to becoming an effective information herder.

Keeping up with the ever-evolving information legal environment

When all the company business activities and related information are identified through your BPA, it will be essential to understand the laws and regulations that apply to them and what it takes to comply with those rules.

To deal with the ever-evolving information legal landscape, companies should have a process in place to monitor changes in the law and incorporate those changes into policies and procedures to ensure that data compliance is up to date. One company we worked with called this process CIT—the Compliance Implementation Team—made up of legal, compliance, business, and operations representatives who collaborated to educate business units on these changes, understand what it will take to operationalize them, and then track and document progress in this regard.

Your BPA is the foundation of this effort—informing legal and compliance professionals about what your company does and where. Updating your legal landscape must include regularly updating your BPA as your business activities and jurisdictions change.

Information management is a C-suite responsibility

Executive sponsorship is essential for your BPA and all information-related initiatives with strategic and enterprise impact. If you are a C-suite executive, it is part of your fiduciary responsibility to understand your information assets and associated risks. If you are not in the C-suite, you need to help those senior leaders recognize that their sponsorship of all such initiatives will be necessary to get buy-in and effect change across the enterprise.