SECURITY BOULEVARD

With CCPA Approaching, Is True Data Deletion Possible?

by Sue Poremba on February 26, 2019

For consumers, the proliferation of data privacy laws means control over their sensitive information once they share it with a company (or at least the appearance of control). For organizations, data privacy laws can be a logistical nightmare. How do you delete all of this data to meet regulation requirements while keeping business operations running smoothly?

The UK's General Data Protection Regulation (GDPR) brought the concerns of data privacy to the forefront. Next, the California Consumer Privacy Act (CCPA) is bring data privacy to the home front. While other states have some data privacy laws either in effect or going through the legislative system, CCPA is the one making the biggest splash, probably because if it affects Californians, it will trickle down to affect all of us. Because of that, data deletion is something every organization is going to have to address in the coming year—and deleting that data will not be an easy task.

I spoke with Kon Leong, CEO of ZL Technologies to get his perspective on the struggle to delete data and be compliant with CCPA and other privacy laws.

Ownership of Data Belongs to Consumers

There are a few differences between CCPA and GDPR. CCPA allows 45 days rather than one month; there is a different list of exceptions; and of course, CCPA applies primarily to California residents. But, Leong pointed out, "at their core, they both pose the same fundamental challenge: finding and deleting personal data relating to the data subject. In a sense, these regulations effectively move ownership of data from the enterprise to the individual, which represents a paradigm shift in the way we view data management."
Yet, consumers aren't in total control and can't have their data deleted on a whim. So while organizations bear the responsibility of deleting someone's personal information, there are some exceptions to when they must do it. For example, said Leong, GDPR makes exception for data needed for "legitimate interests," which actually poses a whole new challenge of determining whether data can, in fact, be deleted. "There is a hierarchy of deletion prioritization which must be enforced over legal, compliance, records-keeping and privacy

needs," Leong added. "Sorting out the order of these requirements will cause quite a few headaches itself and represents even more convincing reason why data must be managed holistically."

Data in the Silo

The challenge for most companies in deleting data is where that data lives—in silos. It's the way IT architecture is set up—and that, in turn, creates a technology challenge for an organization's ability to comply with privacy regulations.

"Personal data lies scattered across enterprise repositories such as file shares, SharePoint sites, email, various management platforms, etc.," said Leong. "A key problem is that these repositories are often managed in isolation from one another—i.e., in silos—and the regulations are very clear: Privacy regulations respect no silos. So, organizations are now faced with this new challenge of searching, managing and remediating data across silos, a task that has bedeviled IT since its inception."

According to Leong, the deletion task is geometrically complicated by the following:

- The resolution of deletion conflicts among various functions such as e-discovery, records-keeping, compliance and privacy.
- The many data media and formats, including the debate over whether and how backup tapes are to be handled when they contain sensitive data.
- The many copies of data that continue to proliferate, including copies made for analytics or third-party outsourced data processes such as e-discovery, etc.
- The very definition of deletion such as whether the deletion is complete upon deletion of the file, the copies, the metadata, or the related index; and so on.

"To what extent regulators will extend forgiveness based on best efforts is yet to be determined, but it appears already that many fiduciaries, including CEOs and board directors, are unwilling to gamble at such high stakes, especially regarding the financial and reputational risk from privacy breaches," he stated. "Organizations should be looking now at proving good faith by selecting solutions that can satisfy the massive scaling and complexity required for privacy."

Will the Data Truly Disappear?

But is it possible for true data deletion? For years we've been told you can delete something, but it never truly disappears. So is there is such a thing as true deletion?

We don't really know. "It's hard to say when duplicate copies lie in repositories across the enterprise," Leong said, "and organizations typically have no comprehensive method of identifying or deleting them.

"However, investing best efforts with the most up-to-date approaches and technologies can go a long way toward mitigating the risk of incomplete deletion," he said.