From the Sponsor

PANEL OF EXPERTS

BIG DATA ANALYTICS

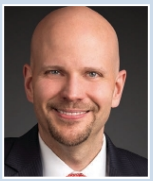
The Dangers of Dirty Data

When it comes to regulation, data can be a dirty word. It has different meanings in different regulatory contexts. There is always more data than one needs, and more than one knows. Data ends up in places where it should not be, is accessed by those who should not do so, and can often defy our best efforts to tame it.

Because of this, any organization leveraging the power of its data must consider proper data hygiene: keeping ever-growing data sets clean, accurate, authorized, and appropriately pruned. Rare is the organization, however, that has a firm grasp on data hygiene, and from a regulatory standpoint, that creates risk.

Case in point, data minimization: restricting intake of data to only what is necessary for the purposes of processing. Data minimization has long been a component of privacy governance frameworks. One of the best ways to protect a person's privacy is to not process that person's data in the first place. Although data minimization has been slow in its regulatory adoption in the U.S., the benefits of limiting your organization's data diet are clear.

If you determine in advance the data elements needed for processing and then only collect those elements, you are well on your way to completing a data classification exercise—identifying and classifying data according to risk and regulatory obligations. If you police your data sets on intake, you also become more aware of data quality issues and data anomalies. At the end of your data lifecycle, a properly minimized data set is easier to identify and delete, when no longer needed for a business purpose.



F. Paul Greene
Partner & Chair of the Privacy & Data Security Practice Group
HSE
Harter Secrest & Emery LLP
ATTORNEYS AND COUNSELORS

Although U.S. laws may not mandate data minimization yet, they certainly incentivize it. The N.Y. SHIELD Act, which came into full effect in March of 2020, focuses intently on getting rid of unnecessary data, with four of its fourteen requirements for an organization's data security program discussing proper data disposal. The recently passed Virginia Consumer Data Protection Act (CDPA), by contrast, requires a Data Protection Assessment—effectively a risk assessment concerning potential processing—whenever a company sells personal information or engages in "processing activities involving personal data that present a heightened risk of harm to consumers." The CDPA does not tell an organization what to do with is Data Protection Assessment, however, other than to hold it for potential review by the Virginia Attorney General. That makes the assessment nothing more than a roadmap for regulatory action, if a problem should ever arise concerning the data set at issue. Yet, if an organization properly limits its intake of data in the first instance, its Data Protection Assessment burden and risk will be significantly lessened.

Despite this, the drive to collect more data, whether it concern consumers or even employees, can be overwhelming. This can lead to bloated, inaccurate, and risky data sets, which are often impossible to manage. Human resources data will almost always be found in an e-mail mailbox, potentially secured by a publicly accessible e-mail address and a reused password. Consumer data may be outdated, incomplete, or just plain wrong.

When an organization suffers a data breach, however, data breach reporting laws, now found in all 50 states, come into play. If the organization cannot identify a consumer or employee affected by the breach, it may have to post a notice of the breach on its website and alert statewide media. Purging old accounts and requiring verification of certain data elements like physical or e-mail addresses up front can help alleviate this risk.

As data proliferates, organizations must align their data hygiene efforts with their risk tolerance. They should no more maintain a risky data set than a risky workplace. Fortunately, a few common-sense exercises—like data minimization, proper data disposal, and maintaining data accuracy—can significantly minimize the risk of dirty data.

Data minimization has long been a component of privacy governance frameworks. One of the best ways to protect a person's privacy is to not process that person's data in the first place.

Raising a shield in your defense

When you're under attack, seconds count. At Harter Secrest & Emery, our battle-tested Privacy and Data Security team stands at the ready, whatever the circumstance. Whether it involves post-incident "breach coach" services or establishing proactive strategies for cyber compliance and incident response readiness, our team has seen it all, from international payment card breaches to local network extortion events. Let our experience help tip the scales of battle in your favor, when dealing with a cyber attack.

Privacy and Data Security

HSE Harter Secrest & Emery LLP
ROCHESTER | BUFFALO | ALBANY | CORNING | NEW YORK CITY

50 Fountain Plaza, Suite 1000, Buffalo, NY 14202-2293

hselaw.com | 716.853.1616

Attorney Advertising. Prior results do not guarantee a similar outcome.