George Kobakhidze, Product Manager, Enterprise Solutions, ZL Tech
May 20, 2021

Share

How to glean user insight while respecting personal privacy

While each person has a unique personality and identity, the digital world has no patience for individuality. The web tries with its every fiber to store, analyze, and classify everything into neat boxes—us included.

To compensate for the idiosyncratic nature of personhood, the digital world meticulously observes and harvests our every action to reduce our complexities down to data points. Invasive websites often know everything from your location, age, income, all the way down to the web browser you use.

As an individual, this can feel incredibly intrusive. However, for these large organizations, a person is simply a row in an overgrown Excel sheet, a small blip in their big data analytics. Begging the question, how can we reconcile the comfort of users with the practices of businesses? Recognizing the humanity behind these data points requires us to bring ethics into these data conversations and analytic processes.

Critically reflect on the current state of sensitive information

The first step in redesigning user analytics is acknowledging that the average privacy and security measures taken on sensitive information are neither private nor secure. Were sensitive information handled ubiquitously with privacy, consideration would be placed first on the user and their comforts and not the benefits to corporations.

It would be culturally unacceptable for a store clerk to follow you around the aisles listening to your every whisper, looking at your texts, tracking where your eyes wander, and noting what you put in your cart—even if the clerk provided helpful suggestions along the way.

However, since this information is virtually housed, these intrusions are dehumanized and tolerated. The mass condoning of data harvesting coupled with the intrinsic value of user data—including sensitive information—has resulted in companies collecting as much data as they can without considering first how to use it or how to manage it securely.

To that end, sensitive information is rarely treated with a security-first mindset. For the most part, organizations treat personally identifying information (PII) the same as other banal data sets, such as the average file or email. Companies often justify this choice by arguing that any rigorous security process would obstruct their analytics functionality.

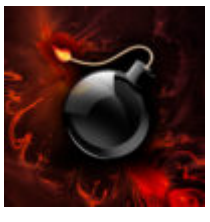
Collaboration between network access brokers and ransomware actors deepens

Why passwordless is not always passwordless

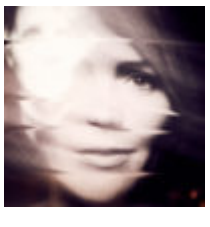
How to glean user insight while respecting personal privacy

What's new

661 fines issued since GDPR became enforceable, totaling €292 million



Collaboration between network access brokers and ransomware actors deepens



How to glean user insight while respecting personal privacy

Application level data protection hindered by misperceptions and complexities

While baseline security practices are decent, they are not impenetrable. In contrast, you can compare these with those assigned to more guarded data, like employee financial documents. These protected files are kept under lock and key and are rarely leaked. Yet, employee financial records are made readily accessible to privileged users as required for regulatory compliance and legal discovery.

Still, most organizations have not adopted these same protections for user data because they are inconvenient and not legally required. The reality is that organizations will continue to use sensitive information. The best we can aim for is an ethical approach.

Center analytics on user privacy and security

Having made these critiques, it is worth noting that there are paths forward that bridge user privacy with analytic functionality. Instead of the “collect it all and deal with it later” approach, organizations should undergo serious discernment to evaluate how to gain the desired insight while treating this data with reverence. Improving privacy and security for analytics that use personal data starts with asking and answering the following questions:

- What are we trying to learn?
- What information do we need?
- How can we protect this data?
- What analyses do we need to run?
- When can we delete the original data?

Drawing a real-world parallel, if you are wondering when your friend’s birthday is so that you can make dinner reservations, it would be strange to ask them what they ate for lunch yesterday, for accesses to their GPS coordinates, and for a copy of their birth certificate. Yet, a simple “When is your birthday?” and “What is your favorite restaurant?” are perfectly normal questions (while still involving personal data). Organizations should create a robust analytics roadmap, from collection to deletion, to manage sensitive information more securely.

A concrete analytics plan enhances user privacy, security, and efficiency throughout data collection, analytics, and deletion. For example, by selectively targeting data for collection, organizations hold onto less personal data and avoid ever ingesting additional sensitive information. Data scientists also save time and increase data security by knowing what analyses to run from the get-go, bypassing the need to decipher what questions to answer from the overabundance of data and reducing the total touchpoints to the bare minimum.

After completing analysis, companies can free themselves of continued data management and reduce the risk of data breaches by purging this information from their storage systems. This process also increases the accuracy of future analytic projects by not relying on old data that misrepresents current sentiments and circumstances.

While each project will require an individualized data privacy plan, the beacons of data minimalization, decreased touchpoints, increased security measures, and early deletion should guide all analytics involving sensitive information.

Approach privacy with newfound urgency

Conversations about sensitive information ethics are burgeoning as regulations like the European Union’s GDPR, the CCPA, and Virginia’s Consumer Data Protection Act (CDPA) put a spotlight on user privacy and security. While these laws are relatively new, they have already made chasmic changes in the ways companies treat privacy.

Since GDPR’s inception, the GDPR Enforcement Tracker has recorded 599 acts of non-compliance, amassing a total of €277,423,288 ($335,279,914) in fines. In years to come, privacy enforcement will only become more rigorous as regulators amp up their oversight and more disparate privacy laws come into play. Organizations can either put in the work to embrace these new ethical guidelines on privacy and security now—or pay for it later.

More about

CCPA cybersecurity data analytics data collection EU GDPR privacy regulation user data ZL Technologies

Share this

Featured news

Collaboration between network access brokers and ransomware actors deepens

Application level data protection hindered by misperceptions and complexities

661 fines issued since GDPR became enforceable, totaling €292 million

Businesses embracing cloud more than ever

3.4 billion credential stuffing attacks hit financial services organizations

Don't miss

Collaboration between network access brokers and ransomware actors deepens

Why passwordless is not always passwordless

How to glean user insight while respecting personal privacy

Endpoint security: How to shore up practices for a safer remote enterprise

The basics o code review

Follow us

- Features
- News
- Expert Analysis
- Reviews
- Events
- Whitepapers
- Industry news
- Newsletters
- Twitter

IN CASE YOU'VE MISSED IT

- How do I select an eSignature solution for my business?
- Sophos XDR: Threat hunting through the entire security ecosystem
- How do I select a managed cybersecurity solution for my business?
- Crystal Eye XDR: Protect, detect and respond to threats from a single unified platform

(IN)SECURE Magazine
ISSUE 68 (March 2021)

- Physical cyber threats: What do criminals leave when they break in?
- Review: Group-IB Fraud Hunting Platform
- Tips for boosting the "Sec" part of DevSecOps

Read online