September 2022

Break Through Barriers to Big Data

How Spectus Accelerates Innovation with Privacy by Design

Big Data: A Double Edged Sword

For leading companies across industries, location data is an indispensable resource that helps uncover behavioral patterns and improve strategic decision making. However, traditional ways of accessing mobility insights are cumbersome, costly, and complicated by legal and logistical factors. Big data is expensive to process—generally $19,000- $25,000 per terabyte per year, and difficult to clean, integrate, and utilize independently within a reasonable time frame.

Location data also carries inherent risks to user privacy, and it is incumbent on the businesses that purchase location data to protect it. A privacy breach has the potential to be disastrous and erodes trust between users, businesses, and data providers. Protecting user privacy is an onerous responsibility that requires businesses to create secure infrastructure, monitor dynamic privacy legislation, and ensure compliance. The lack of a singular universal data privacy law also creates confusion and inefficiencies for data sharing and collection, and while comprehensive federal legislation would help, signing the bill into law is a slow process that is likely years away.

Accessing high-quality location data is further complicated by a lack of supply because providers tend to share their data with few buyers to mitigate the risk of privacy breaches. Without highly sophisticated resources and a skilled team, deriving insights from high volumes of location data can be arduous. Needless to say, businesses are looking for a simpler solution to rapidly innovate with mobility data.

Spectus' Solution: Privacy by Design

At Spectus, our mission is to accelerate innovation by democratizing access to high-quality location data. We're committed to the highest possible standards for privacy protection and operate in a platform-as-a-service ecosystem to safeguard sensitive information, end-to-end. PaaS ecosystems enable granular control over the ways incoming data is processed and accessed by third parties. Operating as a PaaS enables us to implement a comprehensive privacy strategy that's trusted by our partners and data providers and allows us to create an ideal environment for rapid mobility analysis and innovation.

Our privacy strategy is grounded in the 7 principles of Privacy by Design (PbD), a cutting-edge and internationally recognized framework designed to protect consumers' private data while enabling businesses to analyze it responsibly. Abiding by the seven foundational principles of PbD has become table stakes for any company that's serious about privacy.

Spectus' comprehensive privacy strategy empowers partners to transform their business with mobility insights quickly, so they can direct their resources back to the essence of their business—their people and key differentiators.

What is PaaS?

Platform as a service, or PaaS, is a cloud computing model where a provider hosts hardware and software tools on its own infrastructure and delivers both as a service to users for development and analysis. PaaS supplies the data, tools, and guidance for users to build custom solutions quickly. PaaS is valuable because it enables businesses to glean insights from data without the burden of acquiring it and managing privacy compliance in-house.

PaaS ecosystems can also be equipped with state-of-the-art privacy and security measures so users don't need to spend time and resources on complex data minimization processes. CCPA, GDPR, and several other new state privacy laws have made it incredibly difficult to keep up with the changing privacy landscape without a dedicated team of privacy professionals. That's why Spectus takes care of privacy protection for you and allows you to process data quickly and easily in a privacy-first development environment—so you can leverage the power of mobility data without the headaches.

Privacy by Design: Improve Access to High-Quality Location Data

To leverage data responsibly and effectively, there is a growing understanding that "innovation, creativity and competitiveness must be approached from a 'design-thinking' perspective." Design thinking is a human-centered approach that helps businesses develop empathy for their customers. Instead of a means to a single solution, design thinking is a way to tackle difficult problems by continuously evolving and optimizing your development processes.

According to an article in HBR, design thinking has the potential to "unleash people's full creative energies, win their commitment, and radically improve processes." With an increasing emphasis on privacy regulation, a cutting-edge innovative methodology has emerged from design thinking—**Privacy by Design**.

What is Privacy by Design?

Privacy by Design takes design thinking and applies it to technology and business strategy, ensuring that individuals' privacy is protected, especially as technology becomes more powerful. Originally developed by Ann Cavoukian in 1995, the framework was published in 2009 and adopted by the International Assembly of Privacy Commissioners and Data Protection Authorities in 2010. The framework consists of seven foundational principles:

1. Proactive not reactive, preventive not remedial
2. Privacy as the default setting
3. Privacy embedded into design
4. Full functionality—positive-sum, not zero-sum
5. End-to-end security—full lifecycle protection
6. Visibility and transparency—keep it open
7. Respect for user privacy—keep it user-centric

Privacy by Design represents a "significant 'raising' of the bar in the area of privacy protection," and therefore requires technology and implementation that goes above and beyond industry and regulatory standards. At Spectus, privacy is and always has been baked into the core of who we are and what we do, made possible by our stringent privacy framework and data clean room. By operating as a privacy-first platform-as-a-service, we are able to ensure that our data and innovative strategies abide by the seven principles of Privacy by Design.

Privacy by Design: Spectus' Comprehensive Privacy Strategy

1. Proactive not reactive, preventive not remedial

According to the Privacy by Design framework, privacy practices should aim to prevent risks from occurring rather than offering remedies to resolve privacy infractions once they have already occurred. This level of protection requires a clear commitment to enforce the highest standards of privacy—generally higher than existing legal standards.

Spectus' infrastructure proactively protects user privacy and prevents sensitive information from being compromised.

To preserve the privacy of user data, many companies collect sensitive information and then hide it. For example, many SaaS companies collect sensitive information like home addresses and hide them within a CRM to preserve privacy. While hiding sensitive information is proactive, hiding data is not a reliable measure to prevent privacy from being compromised. Hiding sensitive data within a platform is problematic for a few reasons:

- If sensitive data is hidden within a platform, bad actors can find ways to access it.
- In the location space, geographic coordinates are both sensitive & critical information. Hiding geographic coordinates interferes with data scientists' ability to draw meaningful mobility insights.

With the help of a PaaS ecosystem, Spectus created data privacy infrastructure that is both proactive and preventative by enabling differential privacy measures to be applied to incoming data. Differential privacy (DP) is a mathematical definition of privacy – a dataset is said to be differentially private if we can statistically bound the amount of individual-level information an attacker can deduce by looking at the dataset. In addition to multiple governance and processing solutions, Spectus has this state-of-the-art technology in the privacy toolkit.

So how does differential privacy work?

Differential privacy is achieved via a variety of mechanisms that add noise to the process generating the dataset itself. For example, instead of collecting and hiding sensitive data, Spectus applies differential privacy measures to resolve its main weaknesses. We do this by:

1. Removing data captured at locations deemed to be sensitive.
2. De-identifying data as soon as it enters the database. We convert the potentially traceable Mobile Ad IDs (MAID) that enter our platform to encrypted and de-identified Spectus IDs.
3. Minimizing user re-identification by obfuscating home location. Spectus uplevels the coordinates of users' home location to the coordinates of the centroid of the census block group of that area. By doing this, Spectus doesn't compromise users' exact home location and instead indicates the census block group in which they reside.

2. Privacy as the default setting

The PbD framework holds that no action should be required for an individual to protect their privacy —it is built into the system, by default.

Spectus' infrastructure protects personal data in IT systems and business practices, by default.

At Spectus, we believe that consent must be freely given, specific, informed, and unambiguous—we always ask users to opt-in to sharing their location before it is collected. By following an opt-in privacy framework, user privacy is built into the system, and the purposes for which personal information is collected, used, retained and disclosed are communicated to the individual. Furthermore, we ask for geolocation permissions with expanded language beyond the OS standard.

This pillar also specifies that the collection of personally identifiable information should be kept to a strict minimum—also known as data minimization. Spectus does not collect or process personally identifiable information. Our own methodology, **Privacy Enhanced Mobility** (PEM), protects user privacy by mitigating the risk of user re-identification. In order to achieve greater data utility without sacrificing user privacy, PEM improves upon data de-identification techniques by introducing noise to prevent re-identification and further strengthens our privacy protection practices.

What is PEM?

Spectus' patent-pending methodology, PEM improves upon de-identification techniques to protect user privacy. With PEM, Spectus increases privacy preservation while retaining the ability to infer broad user demographics. PEM introduces noise to the inferred home location of users to prevent re-identification by transforming the latitude and longitude values of device location and stops.

3. Privacy embedded into design

According to the PbD framework, privacy should be integral to the system without diminishing functionality.

Privacy is embedded in Spectus' technologies, operations, and information architecture in a holistic, integrative, and creative way without diminishing functionality.

Privacy has been a core value and key element in the development of Spectus. From its inception, we adopted strict privacy compliance—what we called a "privacy-forward" approach. We have been certified by TrustArc, TAG, NAI, and are Privacy Shield registered. We are a charter signatory to the NAI's Enhanced Standards on Precise Location Information. Our data is also GDPR and CCPA compliant, and we are well prepared for the flurry of new U.S. state privacy laws taking effect in 2023.

Throughout its development, Spectus ensured the involvement of all stakeholders by moving critical compliance and risk management activities from siloed departments into the product design process. This cross-functional collaboration is essential to making privacy inherent in the platform and not a bolt-on addition post-design.

All this was accomplished without diminishing functionality—the platform and tools were created specifically to apply privacy principles like data minimization and access control. Privacy was a functional requirement in building Spectus and continues to guide its evolution with each release.

4. Full functionality—positive sum, not zero sum

This PbD principle suggests that the end result must be a win-win scenario—not one where unnecessary trade-offs are made or two important facets are pitted against each other, such as privacy vs. security. It is far more successful to present a positive-sum scenario where both parties come out on top.

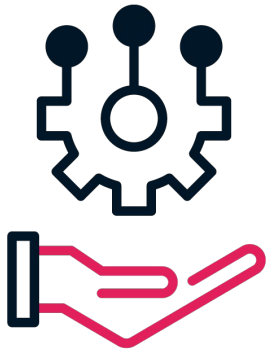
Privacy and security are embedded within Spectus in a positive-sum manner.

Unlike many other PaaS ecosystems, Spectus has industry-leading privacy and security measures already built into the platform. This means data scientists and business executives alike can refocus their efforts on what really matters—their company's own differentiators—rather than using precious resources on data cleansing and processing. With rapid data analysis and intelligent visualizations, teams can rely on the platform to help make informed decisions without compromising functionality or output quality. Therefore, the Spectus PaaS ecosystem presents a positive-sum scenario for all stakeholders.

5. End-to-end security—full lifecycle protection

This PbD principle states that individual privacy, having been embedded into the system proactively, must be continuously protected throughout the entire process. All data should be securely collected, retained, and securely destroyed at the end of the process, in a timely fashion and aligned with user expectations and company disclosures.

Spectus ensures secure lifecycle management of information, end-to-end.



From the moment data enters the Spectus platform privacy controls are applied to its collection, processing, and transformation, ensuring that data and insights are privacy-safe for both the client and the individual. Spectus takes multiple steps to standardize and de-identify data in the platform and ensures confidentiality and integrity throughout its lifecycle. Spectus enforces strict access controls and provides private client tenants to ensure only authorized access to user and client data. All platform access and data processing is monitored and logged. Spectus data is retained and deleted according to our public privacy policy, and client data is securely destroyed upon request.

Spectus ensures the same rigorous standard of privacy protection when transferring personal information to third parties. Spectus' core systems are hosted on Amazon Web Services, which is ISO27001 certified and PCI DSS Level compliant. Data is encrypted at rest and in transit, leveraging AWS private tenants and the Spectus Data Flow Studio to export information securely.

6. Visibility and transparency—keep it open

According to PbD, operations and technology should remain visible and transparent to users to assure all stakeholders that the processes are in fact operating according to what has been stated and promised, subject to independent verification.

Spectus' operations and technologies are accountable, open, compliant, and verifiable.

Spectus hosts all data and users in one central platform which enables us to enforce our privacy policies and governance framework on the end-to-end data flow. We communicate all relevant privacy information available to users in one place—our comprehensive Privacy Center—which includes privacy-related information for all stakeholders, including our Sensitive Points of Interest (SPOI) policy, information regarding privacy rights requests received globally by Spectus and our privacy policy FAQ. Our SPOI policy states that because precise location data is inherently sensitive due to the wealth of information it may provide about consumers' habits and interests, some places are too sensitive to justify in any instance as a privacy-first company. The list of categories can be found on our site.

A truly transparent ecosystem also allows for independent verification of stated privacy protecting practices. Our PEM methodology was reviewed and tested by Oxford Artificial Intelligence (OxAI), a company specializing in Machine Learning and data science techniques based in Oxford, UK. The team at OxAI conducted an independent, rigorous, third-party evaluation of PEM's effectiveness in preserving user privacy. This study found that PEM enhances user privacy preservation, with 88% improvement over industry standards.

7. Respect for user privacy—keep it user-centric

As stated by the IAB, PbD empowers users to "play an active role in the management of their own data," as the individuals themselves "have the greatest vested interest in the management of their own personal data."

Spectus supports user privacy by collecting informed consent, and by providing multiple, simple avenues for individuals to exercise choices such as accessing or deleting their data.

Privacy-protecting measures should not only be user-centric, but also user-friendly. At Spectus, we provide users with several options to easily opt out of location sharing at any time. Located in our Privacy Center, we offer five simple methods for users to opt-out of Spectus sharing, as well as a privacy rights request center where individuals can easily view privacy rights request information and make choices such as opting-out of collection or accessing copies of their data.

Conclusion

In today's information society, harnessing the power of location data is essential to rise above your fiercest competition. Unfortunately, for so many teams on the cusp of innovation, classic big data challenges such as procurement, infrastructure management, compliance, and privacy protection make deriving insights from location data brought in-house prohibitively complicated.

As businesses increasingly rely on third-party platforms for mobility insights, they should be mindful of their ethical and fiduciary responsibility to protect user privacy. By operating as a PaaS, Spectus protects user privacy comprehensively and by default. PaaS affords the flexibility to incorporate the principles of Privacy by Design into technologies and business practices holistically, which facilitates trust with our data partners and reliability with our clients.

Break through the barriers of big data and accelerate innovation, with Spectus.

To learn more about Spectus' privacy policy and how we can help transform your business with location data, contact our team.

spectus™

Data. In Sight.

US Office
45 West 27th Street
3rd floor
New York, NY 10001

www.spectus.ai