THE PII PROBLEM

More regulations. More data. More pressure.

How to master access to personal identifiable information in an evolving privacy climate

OPTIMAL IdM
Identity & Access Management

The problem of controlling personal identifiable information (PII) seems like it should have already been solved. After all, it's not a new issue. But PII leaks are expected to swell in the next few years as businesses expand their investments in the cloud, SaaS, APIs, remote work, and other practices that make every company a partner in a data supply chain, whether it wanted to be or not.

Secrets Sprawl

Data Here, Data There, a Little Data Everywhere

Some regulations require businesses to be able to identify which PII they keep and where they keep it – but a business that uses a cloud services provider (CSP) can't really meet that requirement with confidence. Even if the CSP has datacenters in a specified location, there is no way to know if that provider is outsourcing support to vendors in other countries or using services operated by vendors who are out of compliance with regulations that cover the CSP's customers. A business can trust its CSP, but when the auditors come around, trust has to be verifiable.

A company doesn't have to be using a CSP to fall out of compliance. As DevOps and serverless architecture becomes entrenched in enterprises and mid-sized businesses, chances are high that an IT environment uses a lot of microservices – small pieces of code that perform a single function. Examples of microservices include mapping tools, audio transcribers, mortgage calculators, or any other function that is hard to build in-house but easy to grab from a library or a marketplace.

A microservice developer may or may not be in compliance with PII-relevant regulations, but there's no way to know. And there's no way to know if the microservice developer is storing data that passes through the service or if the data is stored in accordance with regulations. And if a user revokes authorization for a company to use his or her data, there is no way to for the company to be sure if the microservices author has deleted the data or not. Serverless architectures is typically built using dozens or hundreds of these services, so the risk of secrets sprawl becomes unquantifiable, and PII-related auditing gets even harder.

Privacy Regulations

Necessary, Timely, and Hard to Meet

EU-based businesses have had a body of standards to address data concerns called the General Data Privacy Regulation (GDPR) for a few years already. US businesses struggle have tooled up to meet GDPR requirements, but many still fail to comply with one critical aspect: the GDPR requires that PII passed outside the EU be protected by laws as strong as the GDPR. That sounds reasonable, except no other nation-states have data privacy laws as strong as the GDPR. As a result, EU businesses must take extra steps when data can't be guaranteed to reside in the EU.

This is changing. The US is making moves toward stricter data handling laws, and while it will be a few years till GDPR-like regulations are widely adopted in the US, that's the inevitable destination. In order to be well-positioned to meet new requirements when the time arrives, businesses should consider data privacy measures when they make buying decisions over the next few years. To know where to invest, look at GDPR as a guide for how PII should be handled.

As California Goes, So Goes the Nation?

The US Privacy Landscape

In January 2020, California enacted the California Consumer Privacy Act (CCPA), spurred partly by the 2017 breach of a credit reporting bureau that impacted over 140 million consumers. Now, additional consumer protections are being added on via the California Privacy Rights Act (CPRA). The CPRA goes into effect in January 2023, but businesses are required to have the ability to provide personal data reports to California residents twelve months before the law goes into effect – so organizations should already be geared up for compliance today.

CPRA violations will incur penalties of up to $750 per occurrence, with additional fines of $2500 or $7500 per occurrence if the violation was intentional.

Like the GDPR, the CPRA gives consumers the right to know which PII a business has collected about them and how it's being used. They also have the right to opt out of its sale and demand its deletion.

Organizations that already manage HIPAA, PCI, or other regulations may feel that they're ready for the challenges of CPRA. However, the CPRA expands the definition PII to include IP addresses, browser and search histories, geolocation, biometric information, and any other data that could reasonably be linked with an individual. Businesses need to know where this additional information is stored so it can be deleted upon request and they need to protect all of it, even browser data, with the same level of security as they would protect a social security or credit card number.

The CPRA currently affects any business with customers in California, but historically the state has led the nation in technology laws, and where California goes, other states follow. Several other states, including Virginia, Connecticut, and Colorado, either have enacted or are currently considering the enactment of privacy laws of their own.

Federal privacy laws have been discussed as well, but those are not expected to congeal anytime in the near future. That actually makes the situation a lot harder for businesses: without one overarching set of requirements to follow, businesses have to comply with a patchwork of laws. The best approach is to choose the most stringent and comply with that.

How to Manage PII in a Complex Infrastructure

Start with an Identity Access Management solution that already supports GDPR

Strong privacy controls start with the ability to protect PII from unauthorized access or modification and improper use or disclosure. But today's IT environments are so complex that businesses struggle to acquire and maintain visibility into how and where entities – human or machine – access PII. Often, businesses can't even state with confidence whether specific data resides in the cloud or on-prem, or whether PII is hosted in the US, EU, or somewhere else. And a business that doesn't know who or what is accessing its customers' PII or where that data is located is, by definition, out of compliance – not only with privacy regulations, but with many other regulations, including the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and the Gramm-Leach-Bliley Act (GLBA).

Not all IAM solutions include the features necessary to achieve compliance with existing and impending privacy standards. When choosing a solution, the most future-proof approach is to see how a solution helps its customers meet GDPR. IAM can get your log-in data under control, helping you move towards compliance of these standards.

Fundamentals of PII

The following list of capabilities comprise the base level of PII-related competence:

- Consent management gives users the ability to manage their profiles, change their consent settings, and revoke their data.
- Data processing covers security aspects such as the use of encryption and pseudonymization, as well as authentication, authorization, and access management.
- Data minimization is the practice of retaining no more data than necessary, managing it centrally, and partitioning data into different databases so hackers can't steal a full set of PII in one attack.
- Identity governance is the ability to manage user identities across the environment, including visibility levels, access control and security policies, and workflows.

Those are the fundamentals. However, there are other features that are harder to find in the IAM market but are essential for organizations that service customers in the EU and a growing number of US states.

Advanced PII Features

Geolocation

Most IAM providers host their customers' data on shared servers operated by a CSP like AWS or Azure. A customer can't choose a private server or choose the exact data centers where PII will be hosted.

Others refuse to disclose where they host customer data – so when an auditor asks the customer where its PII is stored, it can't provide an answer. Also, a refusal to disclose begs the questions of why they're refusing to disclose. The vendor will likely answer, "Security reasons," but there is no security risk in telling a customer which country its data is hosted in.

Look for a vendor that is able and willing to provide datacenter coverage in multiple regions and allow customers to choose the datacenters where its PII will be hosted.

Best Practice

Choose a vendor that offers private servers and lets you choose a specific datacenter.

Data Flow Control

Today's privacy laws are just the beginning. Not only will more states be enacting their own laws, but new technology is going to raise new issues. A flexible solution is the most future-proof choice.

Most IAM vendors give their customers the ability to geolocate users down to the city level. A rule can be written that lets John Smith only access the network if he is in Dallas, TX. But the rule has to written – and that usually means it is hard-coded, which in turn means it's difficult to maintain and subject to breaking when a conflicting rule is written.

Rules should be writable through a friendly web interface. They also need to be conditional, allowing the business to create rules based on If This, Then That. For example, John Smith can only access the corporate network from outside Dallas during work hours, or John Smith can only access customer PII on Tuesdays. The rules also need to be able to applied to specific apps – so John Smith can access financial data from Dallas on Tuesdays, but can access the company Slack channel at any time from any place.

Auditing and Analysis

An IAM solution should enable detailed reports that allow businesses to view their data in any way they choose and feed it into their analytics processes. Reports should be granular enough to let auditors or forensics investigators see details such as whether a user's account was disabled on the same day that user was terminated.

Data from the IAM solution should integrate with the rest of the security stack and should be exportable to any system. This gives auditors one place to go when they're examining the flow of data. By streamlining the auditing process, audit fatigue is lessened and the cost of audits is reduced.

Geolocation and Context

Browser-based apps have become the norm. When using a browser-based app, the location of the app is the location of the user. That's critical from a GDPR standpoint.

A browser-based app runs scripts right in the user's browser, which is gives the user a richer and more responsive user experience. In-browser execution is also desirable from a developer's point of view for many reasons, one of which is that they often believe that they are not covered by GDPR because they are not handling the data.

Best Practice

Disallow/flag countries that are out of the scope of normal business

What app developers may not understand is that they are joint controllers. They have decided the purpose of the data, they gain a commercial benefit from the processing, they have autonomy over how the data is processed, etc. And any company that offers that app for its employees' use is also a joint controller at that point. If the data is uploaded to corporate databases, the business is then likely to also be a data processor.

For these reasons, GDPR remains relevant in regard to data collected, accessed, or processed in a user's browser.

An IAM solution should be able to limit PII from being sent to specific locations after a user has logged in via SSO. For example, a local credit union is unlikely to ever have legitimate business with an African company and its employees never travel to Africa, so the credit union may wish to disallow all connections from Africa. But what if their bank president does sometimes visit Africa? The IAM should enable the credit union to require multi-factor authentication if the user is outside the US, or in Africa, or in Nigeria, or in Lagos.

Further, the IAM solution should enable businesses to control which PII can go where. Perhaps the bank president needs access to employee PII when in Africa but should never need access to account holder PII. The IAM solution needs to be flexible enough to handle that rule and the rule should be easy to set up through a web interface.

Multi-Factor Authentication

Multi-factor authentication plays a critical role in PII protection, but not only because it makes it harder for bad actors to access data. The CPRA defines login credentials as “sensitive personal information,” and users have the right to private legal action against against a breached company when their email addresses and passwords are exposed.

The encryption of stored passwords give businesses a better chance at meeting compliance, but encryption alone should not be considered enough to protect credentials. For one thing, encryption standards evolve, and for another, more than one company has been surprised to find an old spreadsheet of plain-text passwords forgotten on some server or in some S3 bucket.

MFA is no longer considered “extra.” Today’s IAM solutions almost all offer MFA, but the best choice will be a solution that also allows MFA in context. For instance, customer service professionals at corporate headquarters may not have to use MFA except when they are trying to access PII, and software developers can never access PII at all but do need to use MFA to deploy a new website build.

However, users don’t love MFA, and security professionals will verify that when users don’t like something, they find a way around it. So passwordless authentication is highly desirable, and the more transparent it is to users, the better.

Best Practice

Elevate required authentication with MFA in context

The Optimal IdM Approach: Not just good security. Good data control.

Good security is not the same thing as good data control, and businesses concerned with PII compliance can no longer be satisfied with standard IAM solutions. Optimal IdM gives businesses innovative capabilities that will help them comply with both current and future regulations.

Optimal IdM customers can keep EU customers' data in the EU and US customers' data in the US. That has been a major hurdle for businesses that wish to operate in both markets, but Optimal IdM eliminates some of the friction.

Businesses can control access to PII based on dynamic and static policies built around contextual factors such user behavior, device, location, etc. And not only can they control access to apps, they can control the flow of data to apps, so one user may be able to view all PII in any app while another is disallowed from seeing some or all types of PII in some or all apps.

MFA is included in all offerings, and Optimal IdM MFA isn't just fingerprints and eye scans. The OptimalCloud offers passwordless authentication by supporting Typing Behavior Biometrics, a technology that learns each user's typing patterns so a user doesn't have to use a password at all – they can just type their name or email address to be authenticated.

Optimal IdM is already in compliance with CPRA and meets the geolocation requirements of GDPR. New privacy regulations are not likely to ask for more stringent controls in the foreseeable future, so choosing Optimal IdM today will deliver the best return on investment in coming years. See Optimal IdM in action. Request a demo today – and bring your compliance questions!

Request A Demo Today!

And Bring Your Compliance Questions