

skyflow



The State of Data Privacy 2022

Skyflow's Manish Ahluwalia on Preserving Privacy and Data Workflows



skyflow

Manish Ahluwalia

Ahluwalia has over two decades of experience in the software industry, with over 10 years in information security. He works to help Skyflow's customers find the right architecture for their data protection needs.

Prior to Skyflow, he ran security for NerdWallet.

Data privacy is top of mind early this year, but comes loaded with questions. Is it a CTO or CISO problem? Does securing data make it both beyond the reach of malicious hackers and hard to use for businesses? **Manish Ahluwalia** answers these and other key data privacy questions.

In this interview with Information Security Media Group, Ahluwalia discusses:

- Which executive is most responsible for data privacy;
- The difference between “beyond reach” and “hard to use”;
- How to preserve privacy when aggregating data for analytics.

DATA PRIVACY

TOM FIELD: Is data privacy a CTO or a CSO problem?

MANISH AHLUWALIA: Data privacy in security is everybody's problem. If you're working for a company that holds consumer data, you are

“Data privacy in security is everybody’s problem. If you’re working for a company that holds consumer data, you are responsible for what the company does for the data.”

responsible for what the company does for the data. Different companies formulate different organizations and structures to deal with the bottom-line responsibility for this, but it really should be everybody’s problem – developers, administrators, lawyers, everyone.

SECURITY VS. USABILITY

FIELD: So securing data means putting it beyond reach. Doesn’t that also make it hard to use?

AHLUWALIA: Often, folks do think of security as a trade-off for usability. That’s precisely why you want to think carefully about the right approach to securing your data – one that allows you usability. We think a data vault is the right approach, but however you do it, you have to think about it architecturally so you don’t get into this false-choice scenario.

SENSITIVE DATA

FIELD: You need to secure sensitive data, but doesn’t that conflict with the need to relay that data to workflows, such as issuing credit cards?

AHLUWALIA: You have to think architecturally. A data vault is an architectural package where you store your data in a manner in which it is secured, but it’s also usable, in a way that doesn’t expose your systems to the complexities that come from compliance and regulatory headaches for handling this data. This allows you to execute your workflows on the data while it’s still sitting in the vault. You use the data while it is secure.

A USE CASE

FIELD: Looking at a specific use case, how might organizations looking to reduce the scope of, say, their PCI compliance efforts benefit specifically from using Skyflow?

AHLUWALIA: If you want to charge a credit card, or issue a credit card, depending on whether you’re an acceptor or an issuer, you store the personal information for the consumer or the financial information (credit card number) securely. You execute your workflow in a manner that lets you take the personal information, go to a bank and get a credit card issued, or take the credit card information, go to a payment processor and process the payment

without exposing this data to the systems that should not have access to it. A data vault is a pattern for doing that.

Skyflow's data vault has a feature called Connections that allows you to specify all the details for the connections, with the data living in the vault, and execute this connection to your bank, which is the issuer or your payment gateway, which is your processor, without the data ever leaving the vault. The data will only travel from the vault to the parties that need to have access to it.

WHY SKYFLOW?

FIELD: An organization might ask: If payment card processors such as Stripe can store my PCI data and let me offload compliance, why would I then want to store my data with Skyflow?

AHLUWALIA: If you can find a vendor that solves all your problems exactly the way

you want them, with commercial terms that are agreeable to you, obviously you should use them and not use a platform. But most businesses want flexibility and want to avoid being tied very closely to one vendor. Our platform helps you build integrations with your payment processors, issuers, etc., and it lets you store data that lets you execute your code on the vault itself. You hold onto the data, and you control it. You can execute all your workflows, and you avoid getting locked-in to one vendor.

AGGREGATED DATA

FIELD: How can companies preserve privacy when aggregating data for analytics?

AHLUWALIA: Data is only valuable if you can mash it with more data. The more you mash it up, the more valuable the data is. You need to find out what touch points cross the two sites – the pure analytics side and the use of the data side. Depending on the exact scenario, you need

“Our platform helps you build integrations with your payment processors, issuers, etc. It lets you store data in a vault and execute your code on the vault itself. You hold onto the data, and you control it.”

to architect your solution so that you get both of the best of both worlds – usability and security.

PRIVACY MISSTEPS

FIELD: You see lots of different organizations and sectors. What are the privacy missteps you most often see?

AHLUWALIA: The biggest mistake is assuming data privacy is a problem you can punt. Often, such as when you're starting a project, security is the last thing on your mind. But once your project starts to take off, you have a bunch of data. Data privacy is not something you can bolt onto security. You cannot bolt security on top of an insecure system. The right way to think about this is on day one, but most people don't do that because they think security is the enemy of usability. It is not. The right architectural approach lets you not just store your data securely, but also use it securely in all your use cases and workflows. If you think about this on day one, you can architect an approach that will grow with you. And a data privacy vendor should be able to grow to the use cases and the data volumes that you expect to have.

DATA STRUCTURES

FIELD: How do you look at the different types of sensitive data when designing a vault to secure that data?

AHLUWALIA: Phone numbers and Social Security numbers are data structures with parts. For example, a phone number has an area code or a country code that has meaning to analytics or can determine which telephone vendor you will use to make a contact with this particular user. Data structures have specific meanings.

Skyflow understands that businesses have specific, well-understood flows, on both the business side and the consumer side, and we can give you the right tools, policies and processes to let you execute your workflows without needing to trade security for usability. For example, customers understand that a customer service agent may need the last four digits of the Social Security number to do verification, but they should not need more than that. Skyflow has an out-of-the-box policy where you can give your customer service agents access only to the last four digits.



About us

Every day, we trust our sensitive data with companies to buy medicines, to fly on airplanes, to get loyalty points, to get our salaries and many more. The team at Skyflow is dedicated to ensuring that this data is stored and utilized safely and securely.

Click here to learn more: www.skyflow.com

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

 BANK INFO SECURITY®  Just for Credit Unions CU INFO SECURITY®  GOV INFO SECURITY®  HEALTHCARE INFO SECURITY®

 infoRisk
TODAY®

 CAREERS INFO SECURITY®

 Data Breach
Prevention, Response, Notification. TODAY

 CyberEd.io

**iSMG**
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io