WHITE PAPER

Overcoming CCPA Compliance Challenges

How Graph Technology Powers Consumer Data Privacy Solutions in the U.S. & Beyond

Nav Mathur, Senior Director of Global Solutions, Neo4j`

Overcoming CCPA Compliance Challenges

The new California Consumer Privacy Act (CCPA) takes effect at the beginning of 2020 and imposes stiff penalties on those that misuse and resell consumers' private information. Nevada and New York have also introduced their own privacy regulations. Canada and Mexico, as well as Texas, Washington and many other states are watching the personal data privacy narrative as it unfolds in California.

Using a graph database foundation for your personal data privacy solution places your organization on the fastest, most cost-effective path to CCPA, GDPR and data privacy compliance.

White Paper

TABLE OF CONTENTS

Starting in 2020, companies that collect personal data from Californians are subject to stringent regulations and to penalties for its misuse. And the rest of North America is watching.

Overcoming CCPA Compliance Challenges

How Graph Technology Powers Consumer Data Privacy Solutions in the U.S. & Beyond

Nav Mathur, Senior Director of Global Solutions, Neo4j

Personal Data Privacy Leaps across the Atlantic

American consumers and regulators have been concerned but patient about personal data privacy over the years.

The new millennium brought a tsunami of personal data breaches at Marriott, TJ Maxx, eBay, Equifax, Home Depot, JP Morgan Chase, Target, Adobe, Sony, VeriSIgn, Anthem, Uber and many other major institutions. The top fifteen incidents alone compromised more than two billion accounts. A colossal hack at Yahoo! exposed another three billion identities that appeared for sale on the dark web.

In recent years, the European Union has introduced extensive, strict personal privacy reforms with their General Data Protection Regulation (GDPR), but American lawmakers did not follow suit with their own tighter federal laws.

But when opportunist businesses started to sell the identity of Californians, its state legislature moved quickly to protect its citizens. The most public offense occurred in 2014 when Aleksandr Kogan, a Russian-American professor, amassed profiles for 50 million Facebook users. Only half-a-percent of those account owners consented to the use of their information and only for academic purposes.

Kogan turned the data over to Cambridge Analytica who then repackaged it into targeted digital marketing services that it sold to political campaigns including Donald Trump's presidential campaign. The gravity of this event alerted Americans to the far-reaching and completely unintended consequences of how their personal data can be used.

The new California Consumer Privacy Act (CCPA) takes effect on January 1, 2020. The regulations impose stiff penalties on those that misuse and resell consumers' private information. Nevada and New York have also introduced their own privacy regulations. Canada and Mexico, as well as Texas, Washington and many other U.S. states are actively watching the fallout as personal data protection takes hold in California.

The relationships among the various data elements are the same, regardless of jurisidiction or regulatory terms.

By using a powerful and flexible graph database framework, you easily address the data management requirements of personal data privacy.

What Exactly is CCPA?

CCPA is a set of personal data protection regulations passed by the State of California in 2018 that take effect on January 1, 2020. They address the personal privacy risks associated with the collection, use and resale of personal information about California residents.

The regulations in CCPA require collectors and resellers of personal information to enable California residents to:

- Know which information is collected about them and how it is used
- Examine their information and request its deletion
- Know if any of their information is sold or disclosed, and to whom
- Block the sale of their information, especially for minors
- Enjoy the same level of service whether they opt for privacy or not

If a data breach occurs or a consumer files a complaint, regulators require businesses to document the sequence of events that led to the breach. This requires organizations to keep accurate data lineage records of all private consumer data.

CCPA does not replace existing California privacy laws including CalOPPA, Shine the Light and the Digital World Act's protection of California minors. Existing privacy requirements in CalOPPA and other regulations are still in full force.

CalOPPA applies to all businesses based in California as well as to organizations that collect any information about California residents. It does not require consent to collect personal data unless it belongs to a minor under the age of 16. But CalOPPA doesn't address the resale of personal information.

CCPA adds a layer of privacy protection by requiring businesses to allow users to request that their data is not resold.

Is CCPA Just California's Version of GDPR?

In short: not quite.

In May 2018, the European Union rocked the online world when its General Data Protection Regulation (GDPR) took effect. GDPR's goal is to recognize the realities of today's digital world while giving EU citizens more control over their personal information and privacy.

While the spirit of CCPA and GDPR are similar, there are some important differences. California's CCPA regulations are focused on the resale of personal information while GDPR requirements are wider and more far-reaching.

Do I Need Separate Solutions for CCPA and GDPR Compliance?

There is some good news in this complex wave of new privacy regulations: The data issues underlying CCPA, GDPR and other privacy regulations are very similar. The relationships among the various data elements are the same, regardless of jurisdiction or regulatory terms.

By using a powerful and flexible graph database framework, you easily address the data management requirements of personal data privacy, no matter the origin of particular regulations.

Organizations that embrace the new privacy regulations and provide the right levels of transparency and traceability for personal information have a big opportunity to win the hearts, minds and business of California consumers.

Personal Data Privacy Raises Difficult Questions

To meet the personal privacy requirements of CCPA, GDPR and other regulations, you must be able to answer these difficult questions:

Data Elements	What data do you have?	Where is the data stored?	Why do you have the data?
Data Sources and Uses	How and when did you obtain the data?	How does the data travel through your systems?	Do you have permission to use the data? For what purpose?
Data Security	Is the data secure?	Who has access to the data?	Does the data ever cross international borders?

But the new privacy demands don't end there.

You must know when and where breaches occur and what data was taken. You have to give people a way to view their personal data and how it's being used. You also must give them the abililty to limit its use, prohibit its sale, or even delete their personal information. Perhaps most importantly, you must be able to prove to regulators that you are in compliance with personal privacy requirements.

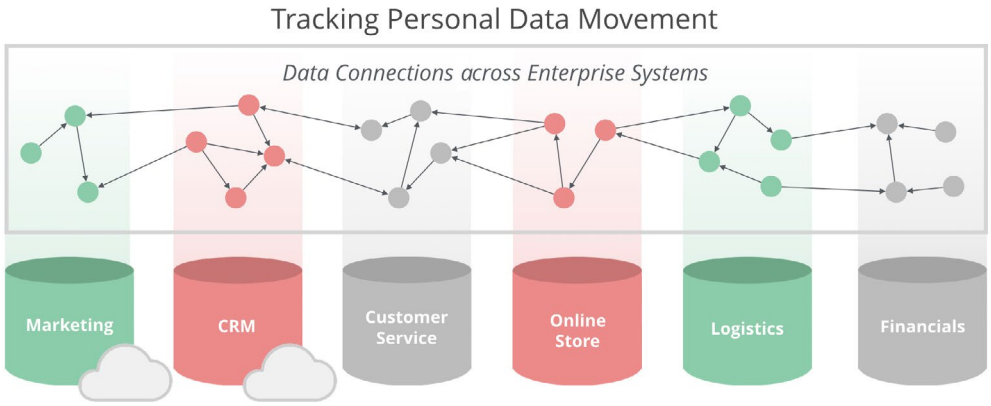
CCPA and GDPR are the most far-reaching and technically-demanding data privacy regulations ever established. While they surface significant data management challenges, they also provide a great opportunity for forward-thinking organizations. Enterprises that embrace the new regulations and provide transparent tracking of personal information have a big opportunity to win the hearts, minds and business of consumers.

To solve privacy challenges, you must be able to track personal data movement across all internal and external systems – even as your systems and workflows change.

Tracking Personal Data Requires Deep Visibility

In modern organizations, personal data resides in many applications that span servers, data centers, geographies, internal networks and cloud service providers. Regulators hold you accountable for that data regardless of where it is stored. And you must be able to access, report and remove personal information from all those systems when required by consumers or regulators.

To satisfy privacy requirements, you must be able to track the movement, or *lineage*, of a contact's personal data – where it was first acquired, whether consent was obtained, where it moves over time, where it resides in each of your systems, and how it gets used. The connections among those systems and silos are key to tracking the complex path that personal data follows through your enterprise.



The key to personal privacy compliance is tracking data movement across all your enterprise applications

Graph Databases Are the Right Foundation for Data Privacy Compliance

Personal data seldom travels in a straight line and instead follows an unpredictable path through the enterprise. That path is best visualized as a graph, so it's not surprising that personal data problems are best addressed by a graph database. Graph technology is designed for connected data applications in which data relationships are as important as the data itself.

As the leading graph database platform, Neo4j includes powerful data visualization tools that enable you to model and track the movement of sensitive data through your systems. As a result, you provide easy, clear answers about personal data to:

- Regulators who demand proof of privacy compliance
- Data protection officers and internal staff responsible for preserving privacy across all your systems
- Individual consumers who ask what you know about them and how you are using their data

Why Graph Technology Is Superior for Privacy Compliance

The complex data lineage problems posed by privacy regulations are impossible to solve with relational and most NoSQL technologies. A modern graph database platform like Neo4j is a superior foundation for addressing the connected data requirements of privacy compliance.

RDBMS Cannot Handle Connected Data

Relational database (RDBMS) technologies are built for managing highly structured datasets that change infrequently and have minimal numbers of connections.

To connect all your private personal data, you need a colossal maze of JOIN tables and many thousands of lines of SQL code. Those queries require several months to develop and are nearly impossible to debug and maintain as you add more systems and data relationships. Most importantly, queries of such complexity take hours to days to execute and easily hang your server.

Non-Native Graph Technologies Break Down

Some NoSQL and relational databases claim to have graph capabilities. In reality, they have cobbled a graph layer onto their non-graph storage models.

These non-native approaches inevitably omit key system connections and break personal data lineage, making them easy targets for regulators. Neo4j is a native graph database that stores and connects data as a graph – just as you visualize it – making Neo4j the ideal technology for privacy compliance.

A Picture Is Worth a Thousand Words: Proving Privacy Compliance

The ultimate test for any personal-privacy technology is its ability to satisfy regulators and consumers that your organization is in compliance.

Traditional approaches produce tabular output that is hard to trace. In contrast, Neo4j produces simple, easily understood visualizations of how personal data flows through all your systems.

A Modern Graph Approach Is Superior for Privacy Compliance

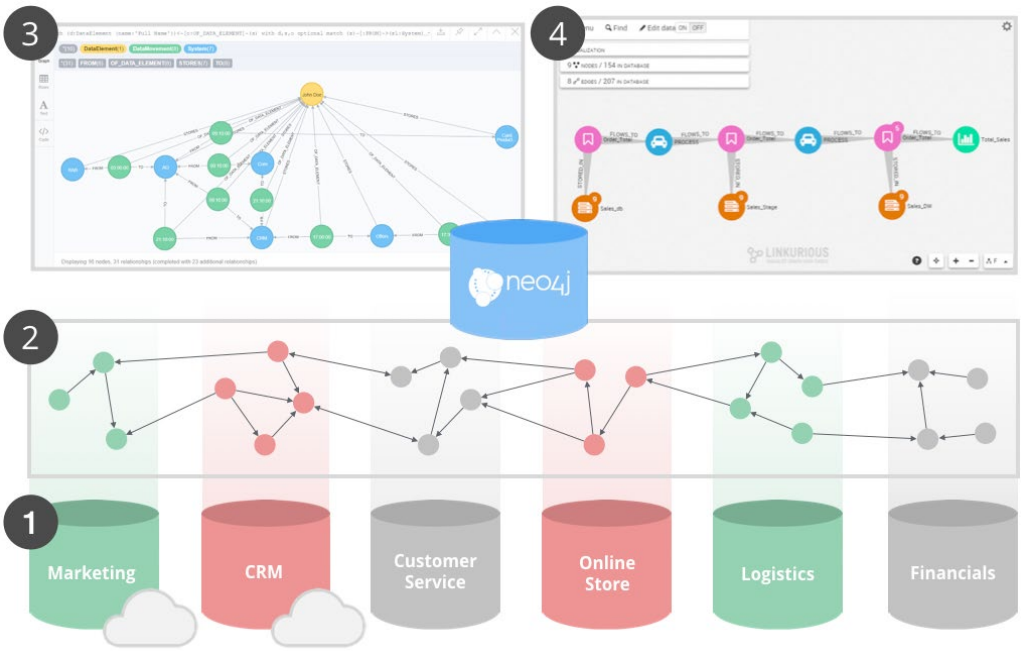
Privacy Task	Traditional Approaches	Modern Neo4j Approach
Trace data through enterprise systems	Complex queries with hundreds of JOIN tables	Simple, single query traverses all enterprise systems
Preserve the integrity of data lineage	Broken data paths and lineage, especially with NoSQL databases	Continuous, unbroken data paths at all times
Effort required to add new data and systems	Days to weeks to rewrite schema and queries	Minutes to draw new data connections
Time to deployment	Months to years	Weeks to months
Response time for compliance requests	Minutes to hours per query	Milliseconds per query
Form of compliance responses	Text reports that are not visual and prove very little	Visuals of personal data and the path it follows through your systems
Bottom line	**Long, ineffective and expensive**	**Easy, fast and affordable**

Personal data connections are impossible to track with traditional SQL and NoSQL databases, making them poor foundations for addressing privacy compliance challenges.

Using Neo4j, follow these simple steps to plan, create and use a data privacy solution that tracks the flow of personal information across your entire enterprise.

Four Steps to Personal Data Privacy Compliance

Follow these steps to build your organization's personal data privacy solutionusing the Neo4j Graph Platform as its foundation.



STEP 1 Inventory Your Systems

Identify all enterprise systems that use or could potentially use private personal information. Document where and how those systems store personal data.

STEP 2 Build Your Logical Data Model

Build a logical model of personal data elements, and how and when they flow across your systems. Define system connections including metadata that describes and quantifies them.

STEP 3 Develop and Test Your System

Using your logical data model, load your data into Neo4j. Then leverage Neo4j's Privacy Shield Framework to develop and test your solution by creating simple queries and reports that address personal data privacy requirements like CCPA and GDPR.

STEP 4 Visualize and Respond to Compliance Requests

Use the Neo4j graph database and data visualization tools like Neo4j Bloom to display the flow of personal data across your systems. Quickly answer questions from regulators and consumers alike about how personal data is being used by your organization.

Overcoming CCPA Compliance Challenges

Neo4j provides a privacy framework alongside professional services that place you on the fastest, most cost-effective path to personal data privacy compliance.

Complete Privacy Compliance Solution

Privacy regulators in Europe and North America are dead serious about protecting the privacy of their citizens' personal data – and you should expect the rest of the world to quickly follow suit.

CCPA, GDPR and other data privacy regulations mandate strict compliance and call for steep fines for violations. So selecting the right privacy framework is crucial. It needs to manage private data relationships natively, provide a foundation for capable, fast deployment and be customizable to meet the precise needs of your organization.

With the leading graph database and our Privacy Shield Framework, Neo4j propels your organization down the fastest, most cost-effective path to personal privacy compliance so you can:

- **Trace the lineage of regulated personal data** from its acquisition through every system across your enterprise
- **Modify your privacy solution as your business changes** without disrupting existing data and systems
- **Perform ad hoc compliance queries** in milliseconds for fast response to requests from regulators, business managers and consumers
- **Deploy your solution efficiently** with 10 times less server hardware
- **Show regulators visual compliance proof** of personal data flows and lineage across your systems
- **Earn the trust of your customers** and establish your organization as a customer advocate and modern industry leader

Take The Next Step in Privacy Compliance

Neo4 delivers a custom, comprehensive compliance solution for CCPA, GDPR and other personal privacy regulations in as little as four months.

For more information about the Neo4j Personal Privacy Shield framework, visit:
http://neo4j.com/resources/neo4j-privacy-shield-data-sheet/

To learn more about how Neo4j helps you comply with privacy compliance or to request a demo, visit:
http://neo4j.com/use-cases/privacy-risk-compliance/

Or if you would like to discuss a specific initiative, please contact Neo4j and schedule a meeting with Nav Mathur.

Neo4j is the leader in graph database technology. As the world's most widely deployed graph database, we help global brands – including Comcast, NASA, UBS, and Volvo Cars – to reveal and predict how people, processes and systems are interrelated.

Using this relationships-first approach, applications built with Neo4j tackle connected data challenges such as analytics and artificial intelligence, fraud detection, real-time recommendations, and knowledge graphs. Find out more at neo4j.com.

Questions about Neo4j?

Contact us around the globe:
info@neo4j.com
neo4j.com/contact-us