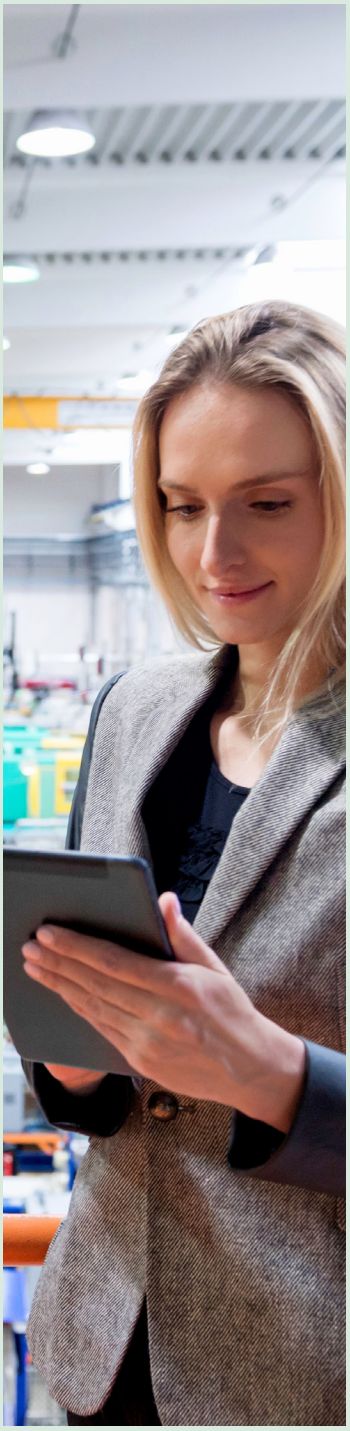
WHITE PAPER



TACKLING IOT DATA PRIVACY FOR MANUFACTURING SECTOR

Abstract

Adoption of digital technologies has gained momentum in manufacturing sector and this new wave digitalization is acknowledged as fourth industrial revolution i.e Industry 4.0. Industry 4.0 is the term coined for the automation and data exchange taking place in manufacturing sector. The core aspect of Industry 4.0 is Internet of things. Internet of things is connection of physical devices to internet and to each other with objective to collect and transfer data. IoT applications has opened large areas of opportunities across manufacturing value chain but has also posed some concern related to personal data privacy. Organizations are working towards finding ways to deal with data privacy challenges in IOT ecosystem and with introduction of some of the privacy laws like GDPR , CCPA , this has added another dimension of regulatory compliance as well.

This whitepaper focuses on how IoT has transformed manufacturing sector, what are the privacy challenges related to data captured by IoT devices and how these challenges can be tackled in order to be compliant to some of the Privacy laws.

Infosys®
Navigate your next

TABLE OF CONTENTS

Introduction

Currently manufacturing industry is going through fourth industrial revolution, which is coined as Industry 4.0.

IoT is the main corner stone for this revolution, which is about connecting everything using smart devices. IoT generates tons of data, which brings focus of industry to data security and data privacy principles and practices.

The existing IoT framework prevailing in the industry takes care of the security aspect of data like encrypted transmission, device authentication, identification and cutoff of malicious and tampered devices. But the data privacy aspect is still not catered to by existing IoT framework and is prevailing problem area for manufacturing organizations.

The connected IoT devices exchange huge quantum of data, which also includes personal information. As per the Gartner report of 2017, maximum of the data generated by IoT devices is labeled as 'private' or 'personal'. Newly introduced data privacy regulation by California (CCPA) has given lot of momentum to IoT space, which identifies device IP, IP address as personal identified information. Identifying California household but individual also fall under purview of this act.

Off late post introduction of CCPA IoT privacy has gained lot of traction as regulation has identified IP and device ID as personal identified information. Also, IoT devices which cannot identify individual but a California house hold will also fall under preview of the act.

This whitepaper explains the data privacy aspect in IoT using various popular use cases in manufacturing industry. These use cases are analyzed to understand personal data attributes generated or processed by the organizations and taken as construct to understand or identify the implications of CCPA. The final section of whitepaper present key solution areas and a roadmap to showcase how organizations can become CCPA compliant.

IoT use cases in manufacturing:

As predicted by Forbes, manufacturing sector is expected to spend about $40 billion by 2020 on IoT platforms. Below are some of the illustrative use cases of IoT to showcase how it has transformed the manufacturing industry.

- **New feature development:** Manufacturers record and analyze the generated usage data to identify new features of product, which can be needed by customer. The data is further analyzed to prioritize the product features.
- **Product quality:** Organizations are using data from connected devices to identify root cause of product failures. This technique is effectively used in beta testing and thus improving quality of product.
- **Asset tracking:** Asset tracking systems allow an enterprise to monitor and locate their key assets. This helps to manage logistics of raw materials and finished goods. Organizations are able to maintain optimum inventory level and also control theft cases by using effective asset management.
- **Predictive asset management:** Organizations are using data from connected devices to identify when, where and which parts will be needed. This data is used along with inventory data to plan future replenishment and inventory levels.
- **Predictive maintenance:** Organizations are analyzing sensor generated data to predict the failures beforehand. The systems automatically generate triggers to maintenance team and OEM partners. Predictive maintenance keeps systems up and running which helps in cost savings and higher operational efficiency.
- **Connected operations intelligence:** For better decision making and operational efficiency, organizations collect all of generated operational data into a unified system to have real time visibility for systems, people and assets in organization. They can also track employee efficiency and productivity by analysis the jobs performed on machines.
- **Customer analytics:** Organizations are collecting and processing product usage data of customers to identify future purchase needs. This data is also used by organizations to identify cross sell and up-sell opportunities.
- **Pricing and planning:** In order to increase market penetration and revenue top line, organizations are utilizing usage and performance data from connected devices in pricing model. The pricing model outcomes are used by marketing team to create robust segments and differential pricing for the identified segments.
- **Next gen customer service:** Organizations are collecting data from connected products to identify product failure issues and they have developed mechanism to remotely handle the issues. This has helped organization reduce complaint rate at call center and increased first call resolution rate.
- **Fleet management:** Car manufacturers are leveraging GPS data to provide fleet services to companies like Uber. Fleet management services include vehicle tracking, fuel tracking and speed control.
- **Insurance premium:** Many manufacturers are monetizing the data generated by sensors. They are analyzing driving patterns of customers to identify high risk activities which helps insurance companies to identify the premium.

Use case wise data generated and CCPA implications:

CCPA defines personal information as data attributes, which can identify or can be linked to a California resident individual and household. CCPA explicitly calls IP address, device identification number such as IMEI, MAC address, website and device logs as personal information. In order to illustrate how data generated by IoT devices comes under CCPA, we have evaluated above mentioned use cases and identified what type of data is captured and whether CCPA is applicable for that use case. Also we have categorized data subject's as customer, vendor, dealer and employee as per CCPA guidelines.

As mandate by CCPA regulation, organizations need to provide right to know, right to delete, right to access to customers, dealers, vendors and employees. Also if the data captured by IoT devices is transferred to 3rd parties, organizations need to provide right to opt-out to the data subject's. In the below illustration fleet management and Insurance premium are the two use case where 3rd party transfer will occur and hence organization need to provide right to opt-out to customer.

Use cases	Sample data captured	CCPA Implication	Data subject
New feature development	Device identification number, IP address, customer location, search keywords, time stamps , count of login/log out attempts , features usage patterns	Right to know, Right to delete, Right to access	Customer data
Product quality	Product usage logs, customer complaints type, software version, IP address, device identification number, customer email address, Order Id,	Right to know, Right to delete, Right to access	Customer data
Asset tracking	Asset location data, asset weight, asset ID, asset usage data, Vendor code, Order code	Right to know, Right to delete, Right to access	Vendor data
Predictive asset management	IP address, device identification number, customer location, product performance data, customer service history, spare part inventory level, spare part location data, spare part asset ID ,Vendor code , Distributor code	Right to know, Right to delete, Right to access	Vendor data Customer data Dealer data
Predictive maintenance	Machine part performance data, temperature, power consumption, part ID, OEM partners ID	Right to know, Right to delete, Right to access	Vendor data
Connected operations intelligence	Machine part performance data, temperature, power consumption, part ID, Employee id, Vendor code	Right to know, Right to delete, Right to access	Employee data Vendor data
Customer analytics	IP address, device identification number, customer location, product performance data, customer purchase history, purchase id, order id	Right to know, Right to delete, Right to access	Customer data
Pricing and Planning	Product usage level, IP address, device identification number, product performance data,	Right to know, Right to delete, Right to access	Customer data
Next gen customer service	IP address, device identification number, customer location, product performance data, customer complaint data, Time stamp, Call duration	Right to know, Right to delete, Right to access	Customer data
Fleet management	GPS data, IP address, device identification number, fuel consumption data, RPM data, Journey history(Telematics), Age, Sex, Gender, Driving license number , Personal contact details	Right to know, Right to delete, Right to access, Right to opt out	Customer data
Insurance premium	GPS data, IP address, device identification number, break pattern, RPM data, acceleration data, Age, Sex, Gender	Right to know, Right to delete, Right to access, Right to opt out	Customer data

Challenges:

Even when an organization becomes sensitive to data privacy aspect in IoT, organization still faces challenges due to business and IT reasons. Below are key challenges faced by organization for data privacy in IoT:

- **Opaque consent mechanism:** Existing consent mechanism for the IoT devices is opaque is in the form of privacy policies which customer gets while buying products. As per the study most of the customers are not aware what personal data is captured and how organization is using it.
- **Data identification:** IoT devices generate huge volume and variety of information, in most of the scenarios organization capturing IoT data themselves are not sure what categories of data are captured. Approach taken by organization today is to capture all the data and then figure what can be done with data. This approach increase privacy risk as more data means more risk.
- **Various forms of Data** – PII data might not be just restricted to Systems but other areas like Biometrics, Video recordings, Audio recording, Image storage etc.
- **Retention policy:** Another challenge for organization is holistic retention policy, organizations are struggling to identify till what period they should retain data.
- **Offline data capture:** Most of the IoT devices capture information in offline mode also and this has raised alarm as customer data gets captured without knowledge of customer.

Due to above challenges and technical complexity, there is lack of the shelf solution on IoT data privacy. The subsequent section will elaborate key solution areas which organizations need to focus on to tackle IoT data privacy challenges.

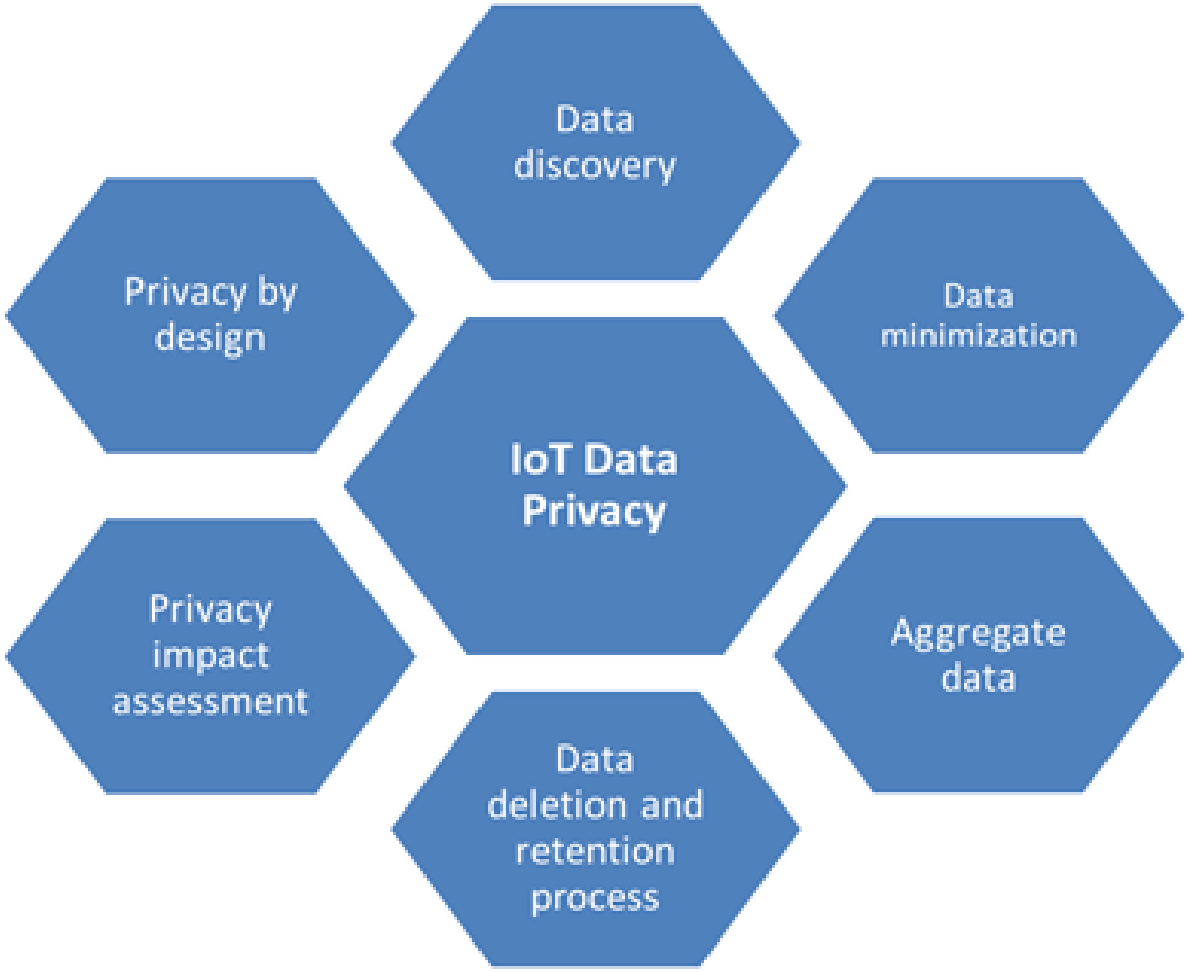
Solution:

IoT data privacy programs are inherently multi-dimensional and touch upon various facets of the organization. For such initiatives, Infosys has created a holistic end-to-end "ADAM" framework, which gives us a tried and tested construct to structure and execute the program successfully. (ADAM here stands for Assess, Define & design, Administer & implement, Monitor & secure).

Assess **Assess, Envision and Roadmap**	***Define & Design*** **Architect, Validate and Design**	***Administer & Implement*** **Build, Test and Integrate**	***Monitor & Secure*** **Stabilize and Improve**
In the assess phase organizations should perform **data discovery** as this forms the building block for IoT privacy program. The objective of data discovery is to uncover all the personal data captured by IoT devices Another key activity which organization need to perform is **privacy impact assessment**. The objective of privacy impact assessment is to uncover all the risk areas in collection, usage and transfer of personal data and create roadmap to mitigate the risk.	In the define & design phase organizations need to identify opportunities for **data minimization, data aggregation**. The objective of the activity is to reduce risk. Another important aspect is policy definition which includes **data retention & deletion policy** and other data protection policy Another main aspect which organization need to consider to tackle IoT data privacy is **privacy by design**. The objective of the activity is to redesign IoT framework keeping privacy by design principles at center stage.	Administer and implement is the phase where organization build solutions to operationalize **data aggregation, data minimization, data deletion and privacy by design principles**	Monitor and secure is the phase where implemented systems are stabilized. The main aspect of the phase to manage the change and provide training to stakeholders. The key objective is to educate stakeholders on how to do business going forward using personal data. In this phase systems are monitored on ongoing basis and areas of improvement are identified

Solution elaboration:

The key solution elements to tackle IoT data privacy challenges are highlighted in below illustration:



Data discovery: Objective of performing data discovery is to identify personal data attributes generated by IOT systems. The solution will identify the impacted applications and help organizations to define future course of action. There are lot off the shelf tools available for data discovery and organizations need to assess which tool best suit to their case. The data discovery tool for IoT data need to have capability to do discovery in unstructured data. Pattern analysis and keyword matching is mechanism generally used by the tools to do discovery in unstructured data. The completeness and accuracy of the tool depends on how well keywords are defined to identify personal data.

Privacy Impact assessment: Privacy impact assessment evaluates organization's IoT data sources, data processing purpose, data flows through service and product lifecycle, data access inventory (to identify who can access data), data retention period and existing IoT data privacy policies. The key objective of this assessment is to identify risk areas against CCPA regulation and to identify severity of the risk. This assessment clearly highlights gaps from people, process and technology perspective and prepare future state roadmap based on identified gaps.

Privacy by design: Privacy by design in IoT puts customer centric approach and takes data privacy principle into account right in the design of IoT products and services. Privacy by design takes into consideration consent or do not collect option, privacy policy notification, opt-out option, guest user identity management while designing IoT products.

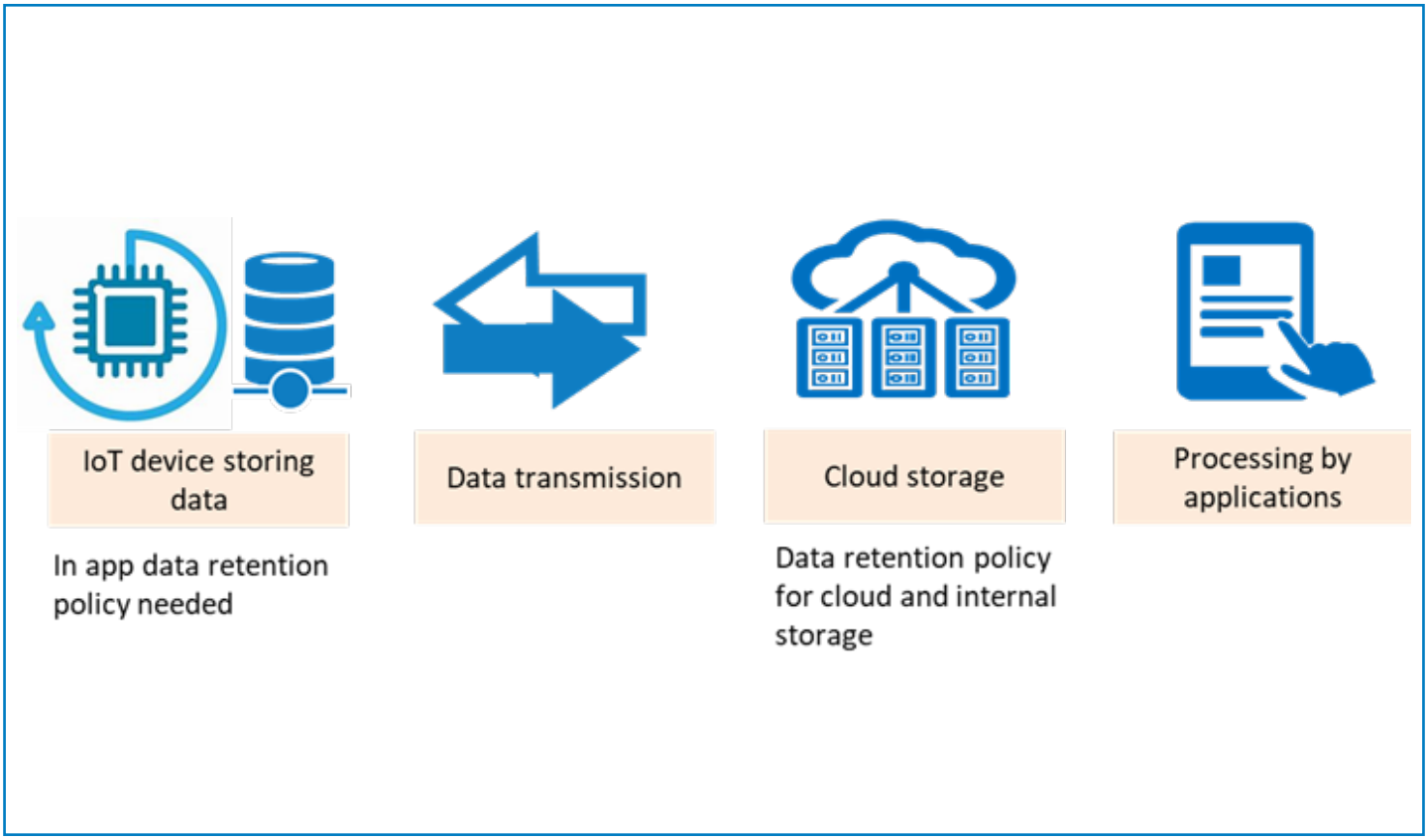
- **Do not collect option:** IoT products can empower customer by providing them switches which can turn off personal data collection. This mechanism will regularize personal data collection and take care of consent aspect of privacy regulation.
- **Privacy policy notification:** IoT devices should have built in privacy policy and should notify customer at

correct timing. Most of the current IoT devices provide privacy policy at first installation. This current practice is not enough in new regulated regime. Organization in the new regime should provide privacy policy at point collection. The privacy policy needs to be contextualized and provide the purpose of collection of information.

- **Opt-out mechanism:** As per CCPA customer has right to opt-out against selling of personal information to 3rd parties. Thus organizations now need to provide opt-out option in IoT interface. Also organization need to ramp up data storage mechanism and should include flag to clearly identify which data sets cannot be transferred to 3rd parties.
- **Identity management:** IoT devices should include functionality of guest user to clearly differentiate device owner from guest user. Guest user on its login should be clearly notified that his usage is tracked and should be given an option to delete his data after usage. IoT devices should also incorporate user identity verification and profile management so one user can access only his information.
- **Customer request mechanism:** IoT interfaces should include functionality from where customer can raise request to know or to delete his personal data.

Data minimization: One of the key strategy to reduce privacy risk is to perform data minimization. The objective of the activity is to identify personal data attributes which are not used in business processes but getting captured at IoT sources. Organizations can reduce their risk by avoiding collection right at the data sources.

Data retention and deletion: Defining data retention period and deleting the data which no more is needed by business is another key aspect of CCPA. As illustrated in the below diagram IoT devices store data in the app as well as data is transmitted and stored in cloud or in house databases.



Thus, organizations should define retention policy for in app stores or cloud in addition to internal storage policy. IoT devices design should include feature of auto data deletion once retention period has lapsed.

For data deletion stored in internal or cloud data bases, organization need to establish mechanism to identify which data has lapsed retention period. To achieve this, organizations to develop business rules to identify inactive devices and develop aging mechanism of data generated by them. Once the data passes the threshold data retention period which is defined as by privacy policy, a trigger is to be generated for data deletion. In order to delete data organization can take a soft delete or complete delete approach. One of the strategy to perform soft delete is by masking IP address and device ID which would be acting as primary key to identify customers.

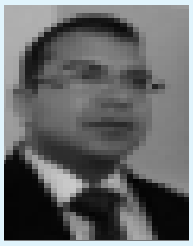
Data aggregation: Data aggregation is the mechanism where organization aggregate data from various customers and use the same for processing and analytics. Organizations can reduce privacy risk by identifying aggregation opportunities and thus can get delete which identifies an individual. In order to opt this strategy organizations, need to understand what type of information and data is consumed in each process and also link the same with purpose of processing.

Conclusion

In this whitepaper we have detailed out key solution components that an organization need to adopt to tackle the data privacy challenge. Out of all the elements, we recommend organizations to start with data discovery to identify what personal data is captured and then take privacy impact assessment to identify gap areas.

IoT data privacy is a multidimensional area and organization need to take holistic systematic and customer centric approach. By taking customer centric approach organization can leverage benefits of IoT and at same time become compliant with privacy regulation.

About the authors:



Gaurav Bhandari *(Senior Principal, Business Consulting at Infosys)*

Gaurav heads the Data and Analytics Consulting practice in Infosys and has extensive experience in management and operational processes, statutory and management reporting, business intelligence and KPI/balanced scorecard and Enterprise Performance Management. Gaurav has played leadership roles in working with senior executives & business users in understanding their business requirements, recommending best practices for process improvement and technology automation, working with technology teams to deliver required business functionality, managed resources, projects in multi cultural environment with effective communication & change management. He also spearheads the data privacy service offerings and has been instrumental in conceptualizing and crafting Infosys data privacy regulations solution and framework.

He can be reached at Gaurav_bhandari@Infosys.com

Aakash Arora *(Industry Principal at Infosys)*

Program management professional with 16+ years of experience in IT Consultancy & Advisory services . He has extensive experience in managing large transformation, Data governance , Data management & compliance programs across the globe for leading organizations . He is currently leading the Data consulting engagements for manufacturing customers & also helping in solution development initiatives for creating new service offerings.

He can be reached at Aakashdeep_Arora@infosys.com

Varun Khanna *(Data Privacy Consultant at Infosys)*

Varun specializes in data privacy implementations, data governance policy definition, and implementation of data privacy measures. He has experience on data privacy laws GDPR, CCPA, and Australia Privacy regulation. He has diverse experience in processes evaluation, data discovery, maturity assessments w.r.t. compliances, defining retention policy, report design, developing executive dashboards, scorecards. He also has rich experience in product management, customer experience and campaign management. Overall he has 6+ years of industry experience.

He can be reached at Varun.khanna02@Infosys.com

Additional resources

- https://www.4cad.fr/content/files/IoT-Use-Case-eBook.pdf
- https://www.cognitiveclouds.com/insights/connected-car-practical-use-cases/

Clearly Opaque: Privacy Risks of the Internet of Things by internet of things privacy forum

For more information, contact askus@infosys.com

Infosys®
Navigate your next