Preserve Privacy When Initiating Your IoT Strategy

FOUNDATIONAL **Refreshed:** 4 December 2019 | **Published:** 13 March 2017 **ID:** G00317400

Analyst(s): Bart Willemsen, David Mahdi

IoT devices generate an unprecedented amount of data, which often includes sensitive personal data. Security and risk management leaders focusing on IoT will need to harness the information gathered for responsible use and distinguish between consumer and business risk.

FOUNDATIONAL DOCUMENT

This research is reviewed periodically for accuracy. Last reviewed on **4 December 2019**.

Impacts

Security and risk management leaders must understand the impact on their organizations now that:

- Organizations are embarking on a wide variety of IoT projects, many of which will involve the collection and analysis of (sensitive) personal data — subject to privacy requirements.
- Existing and upcoming privacy laws, including the EU's GDPR, dramatically impact an organization's strategy, purpose and methods for processing personal data in IoT.
- Many IoT devices will process data in insufficiently protected states, posing significant challenges when ensuring data security and privacy compliance.

Recommendations

Following an organization's privacy management program, security and risk management leaders should:

- Urge IoT stakeholders to include privacy in their risk assessments to:
  - Involve legal advisors to validate regulatory compliance in all business-relevant jurisdictions
  - Identify processing purposes, enabling purposeful use in line with individuals' expectations

- Make an informed decision on appropriate amounts of data needed and purge excess data
- Take a bimodal approach to mitigate privacy risk of data generated by IoT devices and architectures and:
    - Leverage privacy-preserving techniques to enable pseudonymization immediately
    - Select platforms with built-in security features and devices with hardware-backed security
    - Investigate future privacy-preserving techniques, including multiparty computing (MPC), format-preserving encryption, encryption in-use, privacy-preserving analytics (for example, PPSSI), blockchain-enabled use cases, and use of a trusted third party (TTP)

Strategic Planning Assumptions

By 2020, the world will contain over 20 billion IoT devices, generating trillions of dollars' worth of business value.

By 2021, regulatory compliance for critical infrastructure will drive IoT security spend to $1 billion globally, up from less than $100 million today.

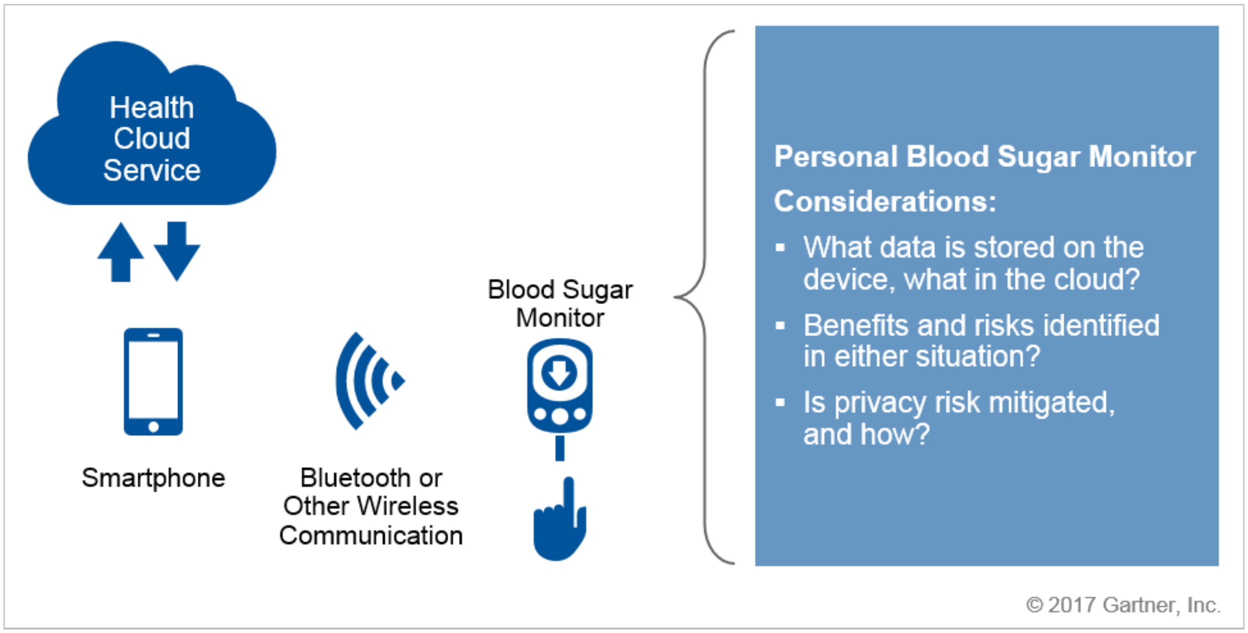
By 2020, 30% of the organizations partnering in Industrie 4.0 initiatives will align their personal data management strategies to overcome end users' hesitations to applying IoT in their daily lives.

Analysis

Whether in healthcare (monitoring devices), the automobile industry (connected cars), agriculture (precision farming) or appliances in the home environment, everything seemingly is connected and generates unsurpassed amounts of data.

For example, a common medical device such as a personal blood sugar monitor (see Figure 1) provides users the ability to read their blood sugar levels accurately, determining the need for subsequent treatment. These monitors may also connect to a personal smartphone, which leverages a cloud service for further analysis/insight. Personal health information can be stored locally and/or in the cloud. This increases the risk to the user and the service provider (which also might be the device manufacturer; see Note 1).

Figure 1. Sensitive Data, Privacy and IoT Devices: Blood Sugar Monitor Example



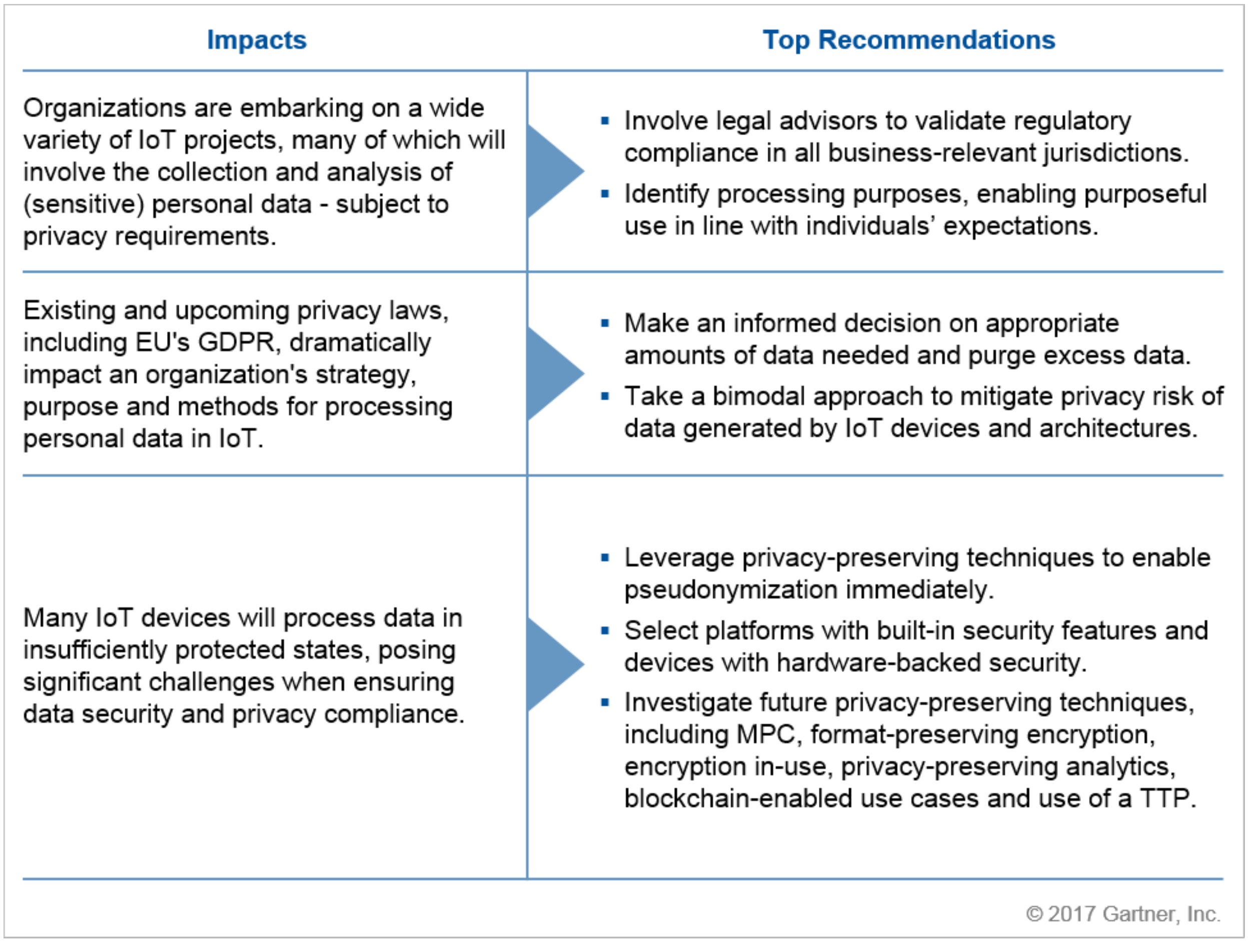
Personal Blood Sugar Monitor Considerations:

- What data is stored on the device, what in the cloud?
- Benefits and risks identified in either situation?
- Is privacy risk mitigated, and how?

Source: Gartner (March 2017)

As regulations and consumer awareness of privacy increase, SRM leaders must base their approach on continuous risk assessment. There is a need for clear guidelines on the retention, use and security of the data. Vendors are (re)starting movement in the area of privacy preserving methods; Clients should adhere to privacy by design in their IoT implementation as a best practice.[1]

Figure 2. Impacts and Top Recommendations for Security and Risk Management Leaders



Impacts	Top Recommendations
Organizations are embarking on a wide variety of IoT projects, many of which will involve the collection and analysis of (sensitive) personal data - subject to privacy requirements.	▪ Involve legal advisors to validate regulatory compliance in all business-relevant jurisdictions. ▪ Identify processing purposes, enabling purposeful use in line with individuals' expectations.
Existing and upcoming privacy laws, including EU's GDPR, dramatically impact an organization's strategy, purpose and methods for processing personal data in IoT.	▪ Make an informed decision on appropriate amounts of data needed and purge excess data. ▪ Take a bimodal approach to mitigate privacy risk of data generated by IoT devices and architectures.
Many IoT devices will process data in insufficiently protected states, posing significant challenges when ensuring data security and privacy compliance.	▪ Leverage privacy-preserving techniques to enable pseudonymization immediately. ▪ Select platforms with built-in security features and devices with hardware-backed security. ▪ Investigate future privacy-preserving techniques, including MPC, format-preserving encryption, encryption in-use, privacy-preserving analytics, blockchain-enabled use cases and use of a TTP.

Source: Gartner (March 2017)

Impacts and Recommendations

Organizations are embarking on a wide variety of IoT projects, many of which will involve the collection and analysis of (sensitive) personal data — subject to privacy requirements about which security and risk management leaders should be informed

Business leaders are drawn into the realm of big data and analytics, all with the goal of deriving business value from client data. Much of the data generated in IoT will be considered "private" or "personal," and therefore requires adequate protection. SRM leaders must ensure that organizations aren't overstepping their bounds when it comes to collection, especially if clients and consumers aren't properly informed. In one example from 2015, Samsung actively recorded conversations.[2] Even if some of these occur under the guise of "feature" enhancements, privacy laws might be in violation. SRM leaders must involve themselves in all of the current and future IoT initiatives to prevent such risks. Ideally, there is an internal reporting requirement for business process owners to inform SRM leaders of new personal data processing intentions in IoT implementations.

Determine the Information, and the Information Life Cycle(s)

Data security enforcement techniques will be dictated by legal and risk constraints as follows:

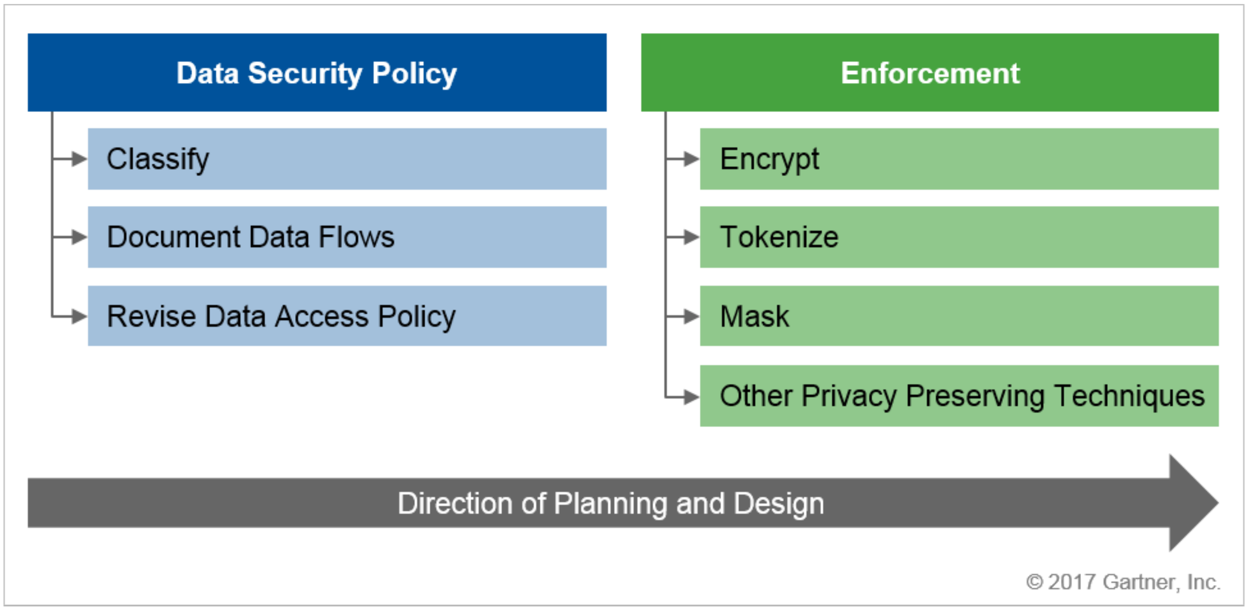
- Regulatory drivers such as industry-specific guidance for health data, payment card data, tracking information, etc.
- Country/jurisdiction privacy requirements, such as the EU GDPR or the U.S. HIPAA (see Note 2)
- General risk assessments and risk tolerance

Device constraints are equally influential. IoT devices come in many shapes and sizes. Devices might possess native security features such as secure elements, whereas others might be simple sensors receiving data to initiate commands (see Note 1 for a definition of device classes). Therefore, native device security capabilities may be limited by device type. SRM leaders need to recommend what devices and/or device designs should be supported to align with business risk appetite.

Ultimately, SRM leaders should join forces with the IoT project owners to begin identifying the data and applying appropriate security controls. In conjunction with Figure 3, it is necessary to:

- Identify data and data flows
- Classify the data and determine the data access policy
- Determine the enforcement technique based on compliance and risk tolerance.

Figure 3. Identify the Sensitive Data and Determine the Appropriate Enforcement



Source: Gartner (March 2017)

Recommendations:

Security and risk management leaders must engage with business stakeholders (see "Use Infonomics to Reset Information Security Budgets") and get involved in all IoT initiatives to:

- Influence design principles
- Ensure personal data generated is adequately protected, taking into account IoT device classes and their (in)abilities
- Determine appropriate method(s) of enforcement, balancing the measure to the risk

Security and risk management leaders should be aware that existing and upcoming privacy laws, including the EU's GDPR, dramatically impact an organization's strategy, purpose and methods for processing personal data in IoT

Jurisdictions such as Australia, Canada and the EU prescribe "purposeful use" of personal data. Determining the reasons for processing personal data is imperative to assess possible compliance hiatus for all business-relevant jurisdictions.

Once processing purposes are defined and documented, it is easy to motivate what data is necessary to achieve that purpose. Data has to be contextually relevant. To mitigate risk from abuse, loss, misinterpretation or other unintended negative results, it is key to control the data life cycle in connection with the identified purposes. A quick method to assess purposes and connected (personal) data to be processed is presented in the "Toolkit: Privacy Impact Assessment Quick Scan."

Rather Than Focusing on Business Risk Alone, Include a Focus on Risk to Individual(s)

It is a misconception to consider personal data as only directly identifiable information, such as a name, (email) address and phone number. Information about usage — and about users — may even indirectly be harmful to an individual if treated out of context. Threats and threat mitigations with regards to all data generated should therefore be identified. Thus, with a specific focus on privacy risk to the individual, IoT architectures should entail subsequent privacy-preserving components.

Pay Specific Attention to IoT Data Analytics

SRM leaders must consider subsequent analytics of personal data already at the initial architecture of an IoT strategy. Pseudonymous information, such as aggregate data processed for analytics, may be kept longer. However, the risk of re-identification will exist in situations where records and attributes indirectly relate to individuals, now or later. Support of the desired business outcome requires legal counsel to determine the appropriate grounds of processing, and alignment with customer expectations (for example, based on consent). In a 2017 example, the FTC sanctioned Vizio for $2.2 million due to gathering users' TV viewing history of 11 million households without proper consent.[3]

Recommendations:

Security and risk management leaders must enable business stakeholders to increase control throughout the personal data life cycle and:

- Assess risks with legal counsel for regulatory noncompliance in all business-relevant jurisdictions
- Define and document data retention schemes in accordance with purpose of use
- Purge excess data at the end of its defined life cycle

Many IoT devices will process data in insufficiently protected states, posing significant challenges to security and risk management leaders when ensuring data security and privacy compliance

IoT devices exist in a variety of forms, spanning the types of device classes, ranging from simple to general-purpose devices. SRM leaders must ensure that the level of security offered by the device matches the business risk appetite in connection with risk assessed in the IoT strategy (see "Hardware Security and Its Impact on IoT Projects"). In "Securing the Internet of Things," Gartner highlights many of the critical areas that SRM leaders need to cover in their security program, such as data flow, threat response or people awareness.

Furthermore, SRM leaders will need to determine if the business aims to launch an IoT initiative on legacy devices or on new custom devices that allow influencing the security design. Each scenario requires a different approach to enable security, and ultimately ensure privacy.

Legacy Devices and Devices With No Embedded Security

One example is an organization that wants to launch an IoT initiative on legacy devices. These devices do not possess enhanced security features or embedded hardware security hardware enhancements.

IoT devices might generate and process data in an unsecured state, such as clear text. Determining possible security enforcements depends on the platform and on the device's OS. SRM leaders will need to investigate at least:

- Available and used protocols.
- Device memory protection, data storage and other aspects such as cryptographic key management.
- IoT device support for third-party software; if available, can they run third-party COTs products or other available security software (that is, run encryption software, support tokenization)?
- For Class 1 devices, it is highly likely that integration with a multifunction gateway is needed. The gateway can introduce compensating security controls and measures (see "Authentication in the Internet of Things").

Custom or Preselected Devices

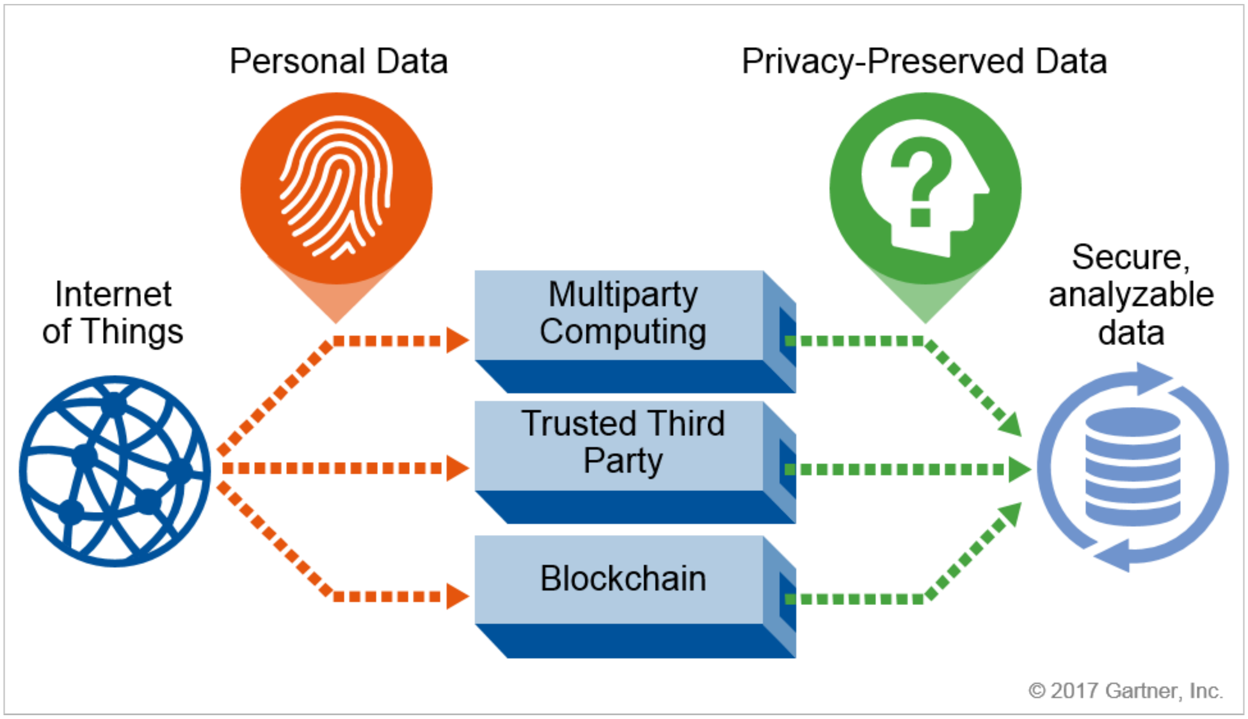
In this case, dictating the IoT devices' specifications is possible. Increasingly, IoT devices are equipped with chipsets that offer embedded security (see "Hardware Security and Its Impact on IoT Projects"). Examples of desirable functions include secure elements, trusted execution environments (TEEs) or trusted platform modules (TPMs; see "Innovation Insight for Trusted Execution Environments on Mobile Devices"). Unfortunately, legacy devices such as the Apple iPhone have the necessary hardware, but currently do not allow third-party access to the security modules. This nullifies the potential gain. Therefore, SRM leaders must determine if the functionality present is accessible. If it is not, these devices must be treated as if there were no embedded security function.

Depending on jurisdictional privacy requirements, IoT devices might need to be equipped with accessible secure elements at an additional cost. Offerings for IoT platforms and IoT security vendors will aim to provide tools to help assess and enforce security and privacy (see "Market Guide for IoT Security").

Emerging Data Security and Privacy Technology

As shown in Figure 4, multiple techniques may be considered to secure privacy in subsequent use of IoT-generated data. Whether tackling legacy or new security enhanced devices, emerging security and privacy technology aims to add further protection to sensitive data.

Figure 4. Leveraging Privacy-Preserving Techniques in IoT Strategies



Source: Gartner (March 2017)

Pseudonymization

Where raw data usually allows for identification, making the information pseudonymous will allow additional use cases in many jurisdictions. Although the risk of singling out still exists and there may be backtracking to source data possible, the privacy risk to individuals is considerably lessened through masking technologies, encryption of records or items, tokenization or a select combination of these techniques.

TTP

Specifically in situations where multiple sources are combined, multiple (source) entities are involved, and/or analysis is performed on sensitive source data, the influence of a trusted third party (TTP) can be relevant. Already considered a relevant addition in certain contexts, a TTP can play a key role in privacy-enhancing technologies (PET).[4] For example, the personal data can be pseudonymized at the source before it is sent to the TTP. Upon receipt, the TTP then performs an additional pseudonymization action. The pseudonyms can be aggregated by metadata characteristics (pseudonyms through which "singling out" is still an option, have then no direct translation to the original index because of the independent guardianship). The resulting information set may be analyzed for predefined reports of which the output then should be anonymous.

Secure Multiparty Computation (MPC)

Known well in academia, MPC is now emerging as a potential method to be applied where sensitive data needs to be mined, shared or processed while remaining in a protected state. While some use cases might apply to data mining (for example, processing data that has already been collected).[5] MPC could be used in IoT security and combined with other methods of cryptography, such as key-splitting. Many data security approaches employ data protection in two main states, at rest and in motion. However, with MPC-based methods and key splitting, it is possible to employ data protection in use. Data protection in use introduces a new paradigm to the arsenal of security methods, and can potentially enhance security for IoT initiatives. The main benefit of data protection in use, when applied to IoT use cases, is that it allows for the protection of data flows without the need to overexpose data.

Currently, use cases are few and far between. The increased international focus on privacy, however, implies a promising era for technologies such as MPC or Apple's differential privacy approach.

Blockchain

Blockchain is a type of distributed ledger in which value-exchange transactions (in bitcoin token, for example) are sequentially grouped into blocks. Each block is chained to the previous block and immutably recorded across a peer-to-peer network, using cryptographic trust and assurance mechanisms. Blockchain-enabled data security applications offer alternative methods to establish trust and resiliency, with little reliance on centralized arbiters, and track digital assets (data types, identifiers, encryption keys, transactions or device attributes). In the realm of privacy, blockchain-based systems offer a paradigm in which users can be in control of their personal data.[6] Any personal data (or references to that data) are secured in a statistically immutable ledger, thus ensuring data integrity. Ultimately, this approach leverages the core benefits of a blockchain-based system, including:

- **Mitigating trust and transparency:** Due to the distributed and decentralized architecture, any change or attempt to change the document is evident and requires consensus among the nodes.
- **Managing and ensuring the integrity of digital assets:** Leveraging the consensus mechanism, the integrity of data is assured since all transactions are digitally signed, and a consensus system is leveraged to mitigate against fraud for example.
- **Enhanced fault tolerance and resilience:** In an ideal blockchain system, if nodes are diverse and distributed — both from a system and location perspective — brute force attacks are mitigated against. As the number of nodes in the system increases, so does the ability to avert faults (see "Innovation Insight for Blockchain Security").

As the excitement with blockchain continues to build, it is imperative to work with developers and architects to establish at least a high-level position on its relevance and a vision for the future adoption. Blockchain-based security and privacy initiatives differ dramatically from legacy business technology and processes. Therefore, SRM leaders should take a bimodal approach and experiment with blockchain-based initiatives as Mode 2 projects.

Recommendations:

Security and risk management leaders focusing on long-term privacy compliance in IoT must:

- Assess possible threats and adequate mitigation, accounting for security posture and risk of IoT devices and architectures
- Determine the IoT devices in scope and adapt to the options for risk mitigation by clarifying if they are legacy devices or new devices where design can be influenced
- Investigate and utilize privacy-preserving technologies such as pseudonymization and take a bimodal approach to investigate future privacy preserving technologies, such as MPC, blockchain-enabled use cases or the introduction of a TTP

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Protecting PII and PHI With Data Masking, Format-Preserving Encryption and Tokenization"

"Roundup of Privacy-Related Research, 1Q18"

"Beyond GDPR: Select and Control Your Service Providers to Ensure Privacy Protection"

"Beyond GDPR: Why Application Leaders Need to Care About Privacy and Data Protection"

"Transfer Personal Data Worldwide"

Evidence

[1] For an overview of the seven principles, see IPC Privacy by Design and Privacy by Design: The 7 Foundational Principles.

[2] See "Samsung's Warning: Our Smart TVs Record Your Living Room Chatter."

[3] See "Vizio to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions Without Users' Consent."

[4] See Dutch DPA opinion

[5] See "Secure Multiparty Computation for Privacy Preserving Data Mining."

[6] See "IEEE Decentralizing Privacy: Using Blockchain to Protect Personal Data."

Note 1 Definition of IoT Device Classes

Current IoT classification methods identify three basic IoT device classes:

- Class 1 devices are simple devices, such as sensors that sense and transmit data, or simple actuators that receive data to initiate commands.
- Class 2 devices are more sophisticated and are able to perform data storage or analysis functions in addition to Class 1 capabilities, such as a simple hub, concentrator or gateway for devices.
- Class 3 devices are sophisticated systems and are much the same as general-purpose servers, which can serve as key aggregation points in an IoT network. Examples include multifunction gateways or security analytics platforms.

See "Authentication in the Internet of Things" for further information.

Note 2 International Privacy Implications

Various standards apply to the management of such data, including the Fair Information Practice Principles (FIPP) and U.S. Health Insurance Portability and Accountability Act (HIPAA). However, in Australia, a court indicated that certain metadata did not qualify as personal information, but other jurisdictions do include this in the definition. In February 2016, a user's IP address and websites visited were considered by the tribunal not to be personal information by the Australian definition, which was confirmed in court in early 2017. For example, in the EU, even pseudonymous information may be considered "personal data" (in 2014, the Article 29 Working Party [WP29] issued a paper on anonymization). IoT devices generate at least indirectly identifiable information, and privacy rights therefore are becoming more relevant at the onset of an IoT architecture implementation.

More on This Topic

This is part of three in-depth collections of research. See the collections:

- Implementing and Executing Your Internet of Things Strategy: A Gartner Trend Insight Report
- Roundup of Privacy-Related Research, 1Q18
- Business Benefits of the Internet of Things: A Gartner Trend Insight Report

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp