Smart Products and Services Adopt a Privacy-by-Design Approach to Build Trust

Abstract

Digital technologies are unlocking unprecedented value for people and businesses. However, in today's connected world, personal data privacy has emerged as a key concern. This is particularly true of products and services powered by the Internet of Things (IoT), as it involves a continuous exchange of data—much of it, personal—among hundreds of devices and service providers. To secure citizens from privacy and data breaches, regulatory bodies the world over are tightening data protection norms. For example, the new General Data Protection Regulation (GDPR) of the European Union, which takes effect on May 25, 2018, is expected to have far-reaching impact on businesses.

This paper discusses the growing need for adopting a privacy-by-design approach to developing trustworthy and regulatory-compliant smart products and services. To harness IoT's true potential, businesses need to embed privacy as a requirement in the design of smart solutions and products rather than providing a privacy feature as add-on.

Introduction

IoT, or the network of physical devices embedded with sensors and connectivity that enables these devices to connect and exchange data, has brought about a "smart" revolution in everyday life. From smartphones, smart refrigerators, and smart cars to smart healthcare and even smart boilers in a power plant—connected devices are opening up new possibilities for businesses to deliver incredible value to users. This network of connected devices runs on the exchange of hundreds of data points, which include personally identifiable information (PII) that is private and, therefore, vulnerable to misuse.

IoT data privacy is a key concern that businesses must immediately and effectively address to deliver trustworthy smart products and services as well as to comply with regulatory mandates. Data protection regulations across regions are becoming stricter to mandate the collection and processing of PII in a verifiable and secure manner. Some of the prominent regulations include, apart from the European Union's GDPR, the UK Data Protection Act, the Federal Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada, Japan's Act on the Protection of Personal Information (APPI), and Australian Privacy Principles (APPs)[1].

User data protection and privacy needs are critical to build trust and enhance consumers' association with smart devices and services. The TCS Global Trend study on IoT[2] that surveyed 795 executives from large multinationals, highlights data privacy as one of the significant challenges for businesses transitioning to new models for smart services. According to a 2017 Gartner report, "Much of the data generated in IoT will be considered 'private' or 'personal', and therefore requires appropriate protection."[3] Gartner also predicts that by 2021, regulatory compliance "will drive IoT security spend to $1 billion globally, up from less than $100 million today."

Data privacy concerns with smart devices and services

Globally, data privacy issues with IoT devices and services are on the rise. A smart TV manufacturer was fined heavily by the US Federal Trade Commission as its devices were found to be tracking TV owners' viewing history and recording it in the company's servers for selling to advertisers without the owners' consent.[4] The German Network Agency has banned certain

smartwatches for children that can record people's conversations in public without their awareness or consent.[5]

Technical design flaws in smart devices, smart services and digital infrastructure can also result in data breach and impact user privacy. The recent census data breach involving 123 million American households has been attributed to incorrectly configured cloud storage.[6] According to the European Union Agency for Network and Information Security (ENISA)[7], smart home applications can profile users by collecting data without their knowledge, which can impact users' behavioral privacy, communication privacy, data and image privacy, location privacy, and privacy of action and association.

Stringent regulations for personal data protection

Gartner predicts that "existing and upcoming privacy laws will dramatically impact an organization's strategy, purpose and methods for processing personal data in IoT."[8] In the United States, the Children's Online Privacy Protection Act (COPPA) mandates as an offense the online collection or maintenance of personal information of children under 13 years, which impact IoT businesses targeting these children. COPPA violators can be held liable for civil penalties of up to $41,484 for each violation.[9] But the most rigorous set of rules that will greet IoT businesses in the European Union from May 25 is the GDPR.[10]

Not only is the GDPR explicit and stringent, but the penalties for nonconformance are severe too, and include steep fines. For instance, Article 7 of the GDPR mandates processing of user data based on consent from the data subject or user, which should be demonstrable by the data controller on request. Article 15 allows the user to access the personal data being processed for the IoT offering and question its purpose. The user can also exercise 'the right to be forgotten' under Article 17(1b) and Recital 65. Under Article 83, businesses noncompliant with the GDPR can be fined up to 4% of their global turnover or €20 million, whichever is higher.[11]

A privacy-by-design approach for IoT businesses

Digital users today do not want to live in an environment where digital outputs are obtained at the expense of personal data privacy. They can raise a variety of privacy concerns to protect

the exploitation of their PII while they use their smart devices. With stricter regulators, businesses also run the risk of noncompliance and penalties. How can IoT businesses address the twin challenges of personal data protection posed by users and regulators alike?

IoT privacy-by-design is a user-centric approach to designing potential smart devices and applications (see Figure 1). It helps ensure that businesses do not fall behind in addressing the data privacy needs of the users and the data protection needs of the regulators, eliminating trust gaps and noncompliance in their smart product/service design.

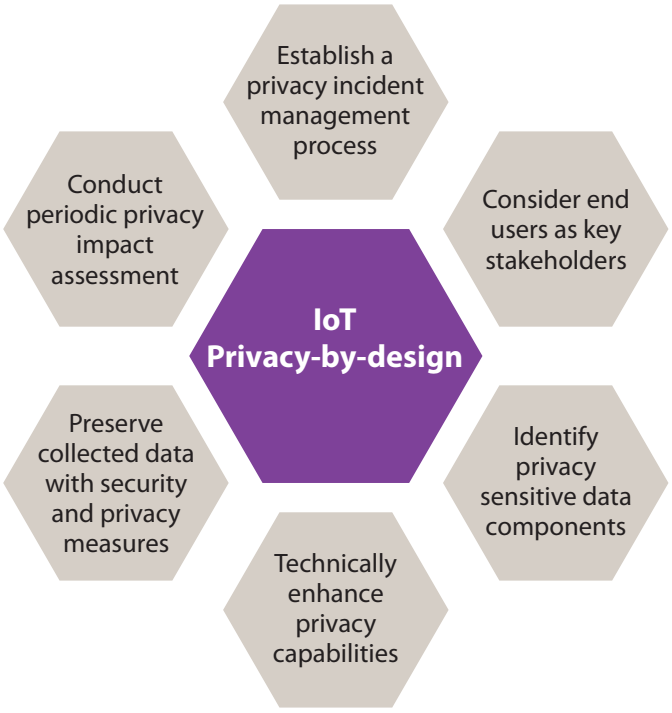

Figure 1: Six steps that drive IoT Privacy-by-design

Privacy by design encompasses IT infrastructure and applications, accountable business practices, and the secured network of sensors. It requires that appropriate technical and organizational safeguards are designed and implemented to ensure protection of not only users' personal data but also the rights of the users to their data. Put simply, privacy by design must ensure that only essential personal data is processed with user consent and no personal data is made accessible without user intervention. The six-step privacy-by-design approach outlined below will help businesses meet regulatory compliance needs, ensure transparency in designing their smart services and products, and make their offerings more reliable and trustworthy.

Step one

Consider end users as key stakeholders of the IoT ecosystem and address their privacy needs in the IoT offering.

Keep the end users' personal data needs and concerns at the core of the IoT device and service designs to build user trust. To do that, IoT businesses should ask if their devices and services provide satisfactory answers to the following queries on personal data usage:

- Are we collecting and sharing users' personal data?
- Which personal data are being collected by the smart device or service?
- Did we obtain users' consent for collecting their personal data?
- With whom are we sharing users' personal data?
- Are we securely storing users' personal data? Is it safe while in use, transit or storage?
- What is our retention policy for users' sensitive data?
- What happens to the stored data after the retention period?
- Do we have a defined process to return or erase user data based on their request?

Step two

Identify privacy sensitive data components in the IoT offering early in design phase.

Design the IoT data flows taking into account stakeholder needs across the application interfaces, infrastructure, and network layouts, so that all the three areas of personal data collection, data transmission, and data processing meet the privacy requirements of the users and the regulators

Step three

Technically enhance privacy capabilities of the IoT devices and smart services.

Embed privacy enhancing capabilities through data masking (such as, pseudonymization) into the IoT device architecture and smart service design. IoT businesses can leverage 'TCS MasterCraft Data Plus Privacy Edition' tool to assist in regulatory compliant data privacy.

Step four

Preserve the data collected for IoT offering with appropriate security and privacy measures. Preserve the contextual data collected by the IoT devices and smart services for safe keeping, using only security and privacy measures that meet all legal and regulatory requirements.

Step five

Conduct periodic privacy impact assessment of the IoT offering to understand privacy risks.

Well-planned, regular privacy impact assessment of the IoT offering will help businesses qualify and quantify all the impacts from privacy shortcomings--in terms of the associated costs of the service or product redesign, financial impact for regulatory noncompliance, damage to reputation, and loss of trustworthiness.

Step six

Establish a privacy incident management process to promptly address sensitive data breach incidents.

Bring data breach incidents to the notice of the business and technical support teams at the earliest to reduce the severity of the impacts discussed in step five. An established privacy incident management process with active response capability will help IoT businesses contain the damages from privacy incidents through prompt mitigation and recovery.

Conclusion

Through the six-step process discussed above, IoT businesses can clearly define and restrict the collection, usage, processing, sharing, and storage of personal data. By placing user privacy needs at the core of the product/service design, the IoT privacy-by-design approach will help businesses devise smarter and ethical products/services, protect user rights, and build the reputation and brand value of their smart offerings, while ensuring full regulatory compliance.

References

[1] Data Protection Laws of the World Handbook, DLAPiperdataprotection.com, retrieved April 16, 2018, https://www.dlapiperdataprotection.com/index.html?c=AU&c2=&t=law

[2] TCS Global Trend Study 2015, Internet of Things: The Complete Reimaginative Force, July 2015, http://sites.tcs.com/internet-of-things/wp-content/uploads/Internet-of-Things-The-Complete-Reimaginative-Force.pdf

[3] Gartner, Make Privacy a Top Priority for Your IoT Project, Nov 14, 2017, retrieved April 16, 2018, https://www.gartner.com/smarterwithgartner/make-privacy-a-top-priority-for-your-iot-project/

[4] Brian Barrett, How to Stop Your Smart TV from Spying on You, Wired.com, July 2, 2017, retrieved April 16, 2018, https://www.wired.com/2017/02/smart-tv-spying-vizio-settlement/

[5] Ellen Tannam, Germany Bans Sale of Certain Children's Smartwatches, Siliconrepublic.com, Nov 20, 2017, retrieved April 16, 2018, https://www.siliconrepublic.com/enterprise/germany-kids-smartwatches-ban

[6] Darkreading.com, Massive Cloud Leak Exposes Alteryx, Experian, US Census Bureau Data, Dec 19, 2017, retrieved April 16, 2018, https://www.darkreading.com/cloud/massive-cloud-leak-exposes-alteryx-experian-us-census-bureau-data/d/d-id/1330673?

[7] D Barnard-Wills et al, Threat landscape and Good Practice Guide for Smart Home and Converged Media, https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-mediaconvergence/at_download/fullReport

[8] Gartner, Make Privacy a Top Priority for Your IoT Project, Nov 14, 2017, retrieved April 16, 2018, https://www.gartner.com/smarterwithgartner/make-privacy-a-top-priority-for-your-iot-project/

[9] Federal Trade Commission, Complying with COPPA, retrieved April 16, 2018, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[10] European Commission, Data Protection, retrieved April 16, 2018, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

[11] European Commission, Data Protection, retrieved April 16, 2018, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

About The Author

Abhik Chaudhuri

Abhik Chaudhuri is a Domain Consultant with the Design and Architecture CoE of Global Technology Practice at TCS, with more than 15 years of experience in IT. He is Chevening TCS Fellow in Cyber Security, Privacy and Policy, and Fellow of Cloud Security Alliance (USA).

Contact

Visit the IT Infrastructure Services page on www.tcs.com

Email: itis.presales@tcs.com

Subscribe to TCS White Papers

TCS.com RSS: http://www.tcs.com/rss_feeds/Pages/feed.aspx?f=w
Feedburner: http://feeds2.feedburner.com/tcswhitepapers

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is an IT services, consulting and business solutions organization that delivers real results to global business, ensuring a level of certainty no other firm can match. TCS offers a consulting-led, integrated portfolio of IT and IT-enabled, infrastructure, engineering and assurance services. This is delivered through its unique Global Network Delivery Model™, recognized as the benchmark of excellence in software development. A part of the Tata Group, India's largest industrial conglomerate, TCS has a global footprint and is listed on the National Stock Exchange and Bombay Stock Exchange in India.

For more information, visit us at www.tcs.com

TCS Design Services I M I 05 I 18