Exponent®

THOUGHT LEADERSHIP

PUBLISHED 1Q 2020

Are Your IoT Devices Leaking Private Data? Tackling Privacy of Things (PoT) Challenges

February 18, 2020

Over 90% of the data that exists today has been generated in the last few years.[1] Every day, Internet users generate 2.5 quintillion bytes of data that must be protected like other valuable assets.[2] While significant emphasis is currently placed on protecting enterprise data, two major trends are driving even more massive privacy challenges in the future: 1) the proliferation of connected devices and 2) the power of artificial intelligence (AI) and machine learning for data analytics and exploitation.

To keep ahead of these trends, avoid common misperceptions about data privacy, and navigate regulatory changes for U.S. and global consumer privacy, device makers need strategies for properly designing, testing, and safeguarding the internet of things (IoT) and its connected components in order to ensure the Privacy of Things (PoT).

The Rise of Connected Devices

The globally installed base of digitally connected devices (IoT) is projected to reach 75 billion by 2025.[3] While the benefits of connectivity are numerous, the challenge of protecting the valuable personal information generated or collected by those devices is paramount. Regulators are increasingly requiring businesses to protect all data, including machine generated data. In one year since the European General Data Protection Regulation (GDPR) and associated enforcement were put into effect, regulators have extensively fined businesses for failing to protect the privacy of European citizens.[4] The fines were assessed world-wide, including against U.S.-based businesses who were deemed to have interacted with European citizens' personal data and failed to safeguard it. Similar laws are now in effect in the United States, most notably the California Consumer Privacy Act (CCPA), which as of January 1, 2020, puts the strictest guidelines in the country on the collection and processing of personal information. In light of these regulations and the associated risks of non-compliance, it is critical for organizations to understand their role in not only protecting enterprise data but also safeguarding privacy and other personally identifiable information (PII) in their products and systems.

Artificial Intelligence Techniques and Privacy

Data generation and collection have greatly outpaced our abilities to analyze and act upon that data. Even today, only a very small fraction of collected data is properly analyzed and applied to inform intelligent decisions. Considering the enormous growth of data, sorting through this information using traditional methods is no longer feasible. In contrast, leveraging AI and machine learning techniques for big data analytics is becoming common industry practice. Organizations are increasingly employing AI and machine learning algorithms and/or neural networks to synthesize data interactions across multiple channels and over time. The use of AI, however, presents another challenge for consumer privacy protection, in particular when AI models act like "black boxes" which are neither transparent nor explainable.

New industry initiatives have emerged in the AI space toward enhancing privacy and security. Notable among these initiatives are federated learning, differential privacy, and multi-party computation. Federated learning trains models on edge nodes before encrypting and transferring them to cloud-based platforms. The end effect is that data stays close to the user while trained models carry all the intelligence without jeopardizing the user's privacy. Differential privacy on the other hand intentionally introduces noise into the data. The noise masks individual information in a manner that still maintains the integrity of the data set as a whole. Multi-party computation distributes a data set over multiple computational nodes such that no individual node has enough personal data to constitute a privacy threat.

The ideal strategy for optimizing AI privacy may differ based on platform, organization, and regulations, but each of these methods shows the potential of AI to make devices more secure and enhance user privacy.

Common Misperceptions About Privacy

One commonly held misconception is that security is equivalent to privacy. A secure system that protects data from external intrusion and malware can still leak data and result in a breach of privacy. Use of personal data by an authorized entity for an unauthorized purpose either intentionally or unintentionally may result in violation of privacy laws. Data privacy also extends far beyond smart phones, tablets, and social media sites. Many of today's smart appliances, home networks, sensors, streaming devices, public networks, biomedical devices, and autonomous vehicles also collect data that must be protected. Unfortunately, the majority of IoT devices currently lack adequate measures to prevent privacy breaches.

Important Regulatory Changes for Consumer Privacy

The CCPA creates new rights for California consumers relating to access, deletion, and sharing of personal information collected by businesses. A business will be subject to the CCPA requirements if it 1) has gross annual revenues in excess of $25 million; 2) buys, receives, or sells the personal information of 50,000 or more consumers, households, or devices; and/or 3) derives 50 percent or more of its annual revenues from selling consumers' personal information.[3] Businesses subject to the CCPA must provide notice to consumers when or before collecting data. Businesses must also create procedures for consumers to opt-out, know, and delete data within specific timeframes.

While the CCPA is limited to organizations who do business with California residents, other states are enacting their own consumer privacy laws. By proactively protecting the privacy of all consumers, organizations can minimize the complexity of state-by-state regulatory compliance and help minimize exposure to future litigation.

The State of California has also approved a bill called SB-327 on information privacy of connected devices. This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified. Other states may follow with similar or more stringent requirements in near future.

Human Factors Analytics

Unfortunately, despite the strongest technical safeguards, human actions, inadvertent or otherwise, often contribute to serious data leaks and PII breaches. Applying a robust human factors testing and assessment program to devices is often the best method of evaluating and mitigating this risk. Human factors testing and evaluations consist of the application of psychological and physiological principles to the engineering and design of products, processes, and systems. The goal of human factors assessments is to reduce human error, increase productivity, and enhance safety and comfort with a specific focus on the interaction between a user and the product. Analysis and testing of human factors therefore should be a key part of the design processes of any system that deals with private or sensitive data.

How Exponent Can Help

Exponent Inc., with our multi-disciplinary groups of security and privacy subject matter experts, design evaluation teams, data scientists, and human factors personnel, has been a leader in the security, privacy, and design consultancy community for well over two decades. We help manufacturers design, evaluate, test, and optimize the security and privacy of products and services to help our clients understand, detect, and mitigate risks.

Exponent also works closely with the legal community to assist with incident response, policy and specifications, litigation support and testifying as subject matter experts.

Are Your IoT Devices Leaking Private Data? Tackling Privacy of Things (PoT) Challenges

Exponent's unique experience in embedded IoT systems enables our firm to perform in-depth privacy and design analyses of end-to-end systems including hardware, chips, sensors, firmware, operating systems, applications, and full-stack protocols. Our early proactive approach helps companies develop products that are secure and compliant to privacy requirements and can ultimately help save more than 50 to 60 times the cost of reengineering the products and services to address post-launch challenges or failures.

Sources:

1 https://techjury.net/stats-about/big-data-statistics/#gref

2 https://www.linkedin.com/pulse/digital-identity-asset-imran-a-hajimusa/

3 https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

4 https://www.intel.com/content/dam/www/public/us/en/images/iot/guide-to-iot-infographic.png

5 https://gdpr.eu/gdpr-fines-so-far/

6 https://oag.ca.gov/system/files/attachments/press_releases/CCPA%20Fact%20Sheet%20%2800000002%29.pdf

7 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327

Brad A. McGoran, P.E., CSCIP, CSCIP/G, GIAC, ACE-M
Statistical & Data Sciences
Principal Engineer
Menlo Park
(650) 688-7013 | mcgoran@exponent.com

Imran Hajimusa
Statistical & Data Sciences
Senior Manager
Menlo Park
(408) 307-2001 | ihajimusa@exponent.com