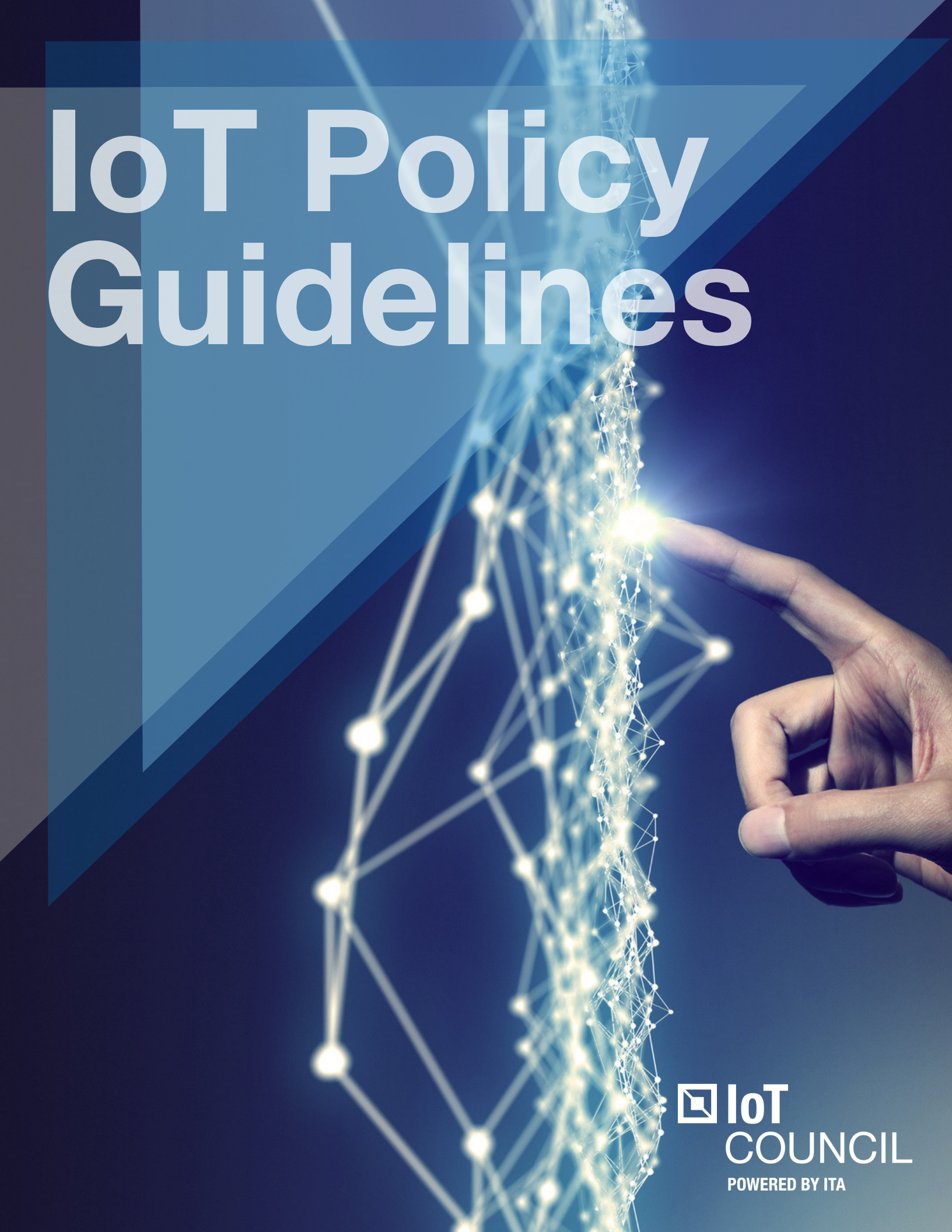
IoT Policy Guidelines



IoT COUNCIL
POWERED BY ITA

Executive Summary

IoT COUNCIL
POWERED BY ITA

Often referred to as the Internet of Things (IoT), billions of smart devices are coming, bringing with them global economic opportunities and innovations that are transforming the way we work, live, and play. The definition of "what is IoT," while still evolving, is far-reaching. What we refer to as the "IoT ecosystem" in this document encompasses this broad concept whether called IoT or not. One of the challenges is for companies to recognize they should have these policies/practices in place even if they don't think of themselves as part of the IoT ecosystem.

As with any modern technology, different components of the IoT ecosystem transition across the maturity curve at their own pace. Many Fortune 500 companies, small and medium-sized businesses and government entities are aiming to transform their business, develop new markets and optimize operations with IoT practices. There is a constant demand to create a reusable and repeatable framework that can enable this realization while continually accommodating evolving business needs and revolutionizing technology into a broad IoT ecosystem in manufacturing, retail, public safety, government, transportation, education and other segments.

The value proposition of IoT is being enhanced continuously with the rapid pace of innovation and exponential growth of the connected devices, diversity of networks, platforms that manage the complete system, data analytics, data lakes, data ponds, security services, mobile applications and end-user services. However, an IoT ecosystem also carries inherent risks due to the evolving nature and sensitivity of data.

The IoT ecosystem is complex, ever-evolving and solving new business needs daily. This complexity is driving a need for guidelines that enable a successful and responsive IoT practice within an enterprise. The IoT Policy Committee of the Midwest IoT Council has developed an IoT ecosystem policy framework covering the following fundamental principles, which can serve as a guide for any business or government entity providing or using IoT products and solutions:

- **Governance**
- **Security**
- **Privacy**
- **Data Management**

The IoT Policy Committee, with its large membership of prominent industry thought leaders, has leveraged experiences in various verticals to create a policy framework that can be adopted by any business (small or significant) or government entity presently in or entering the IoT ecosystem.

Governance

IoT governance policies are tested consistently by the scale and heterogeneity of technologies and devices involved. The area of governance can be as broad or as narrow as needed to ensure that the proper level of administrative guidance and support are in place. Effective governance policies strike a thoughtful balance between participation, accountability, access, privacy, coherence, and safety without constricting innovation and creativity. Governance should consider the aspects and expectations of the IoT producers/owners, applicable federal, state and local laws, statutes and regulations, government and industry policymakers, researchers and civil society in general.

1. Establish a governance committee that includes executive level representation and key stakeholders from various operational, strategic and service functions to provide IoT program direction and oversight.

2. Develop a set of IoT governance policies to address the approach to building, maintaining, securing and supporting the IoT ecosystem.

3. Define the boundaries and interactions between traditional IT structures and emerging operational technology/IoT infrastructure to ensure security and data integrity.

4. Define a set of vision, mission and goal statements for the role of IoT in the enterprise or agency. These become the guiding principles for any decision or prioritization of the IoT opportunities.

5. Define a business case that provides the return on investment for use of IoT, the problem or opportunity statement, key stakeholders, success criteria, expected outcomes and risks. The business case should include the complete list of key performance indicators that would regularly be monitored during the program to track the return on investment.

6. Design the IoT ecosystem infrastructure based on anticipated future traffic and usage, including, but not limited to, communication networks, wireline and wireless modes, internet and satellite connectivity.

7. For any multi-vendor and-or partnership IoT ecosystem, establish formal agreements with internal and external entities that include division of ownership and responsibilities, response windows, data protection, security and mitigation expectations and compliance enforcement. Establish reporting, remediation processes and protocols. Establish a timely schedule to review and update these agreements as applicable.

8. To address the rapid evolution of an IoT ecosystem, establish a prompt review schedule to re-evaluate the business case, tackle updated laws and regulations, audit and refresh technology, initiate modular upgrades, apply industry best practices and mitigate new risks. Wherever possible, future-proof the IoT ecosystem while addressing and supporting past versions and releases.

9. Since many legacy systems and processes are not prepared to confront the privacy and security risks that IoT ecosystems invariably face, develop a method to evaluate, prioritize and bring at-risk legacy systems into compliance.

10. Establish monitoring and measurement criteria for the performance and operational excellence of the IoT ecosystem. The governance committee shall regularly provide operational oversight to monitoring these metrics.

11. Establish a defined set of grades or classifications for the IoT components for the security, privacy and vulnerability of the IoT components, driven by risk impact analysis.

12. Establish an IoT ecosystem that is based upon open architecture, open standards, inclusive design, standard protocols, interoperability, modularization and multi-component sharing principles.

13. Apply a best practice approach to developing the IoT digital components. Design all digital or vulnerable elements to be updatable and patchable. Utilize passwords that are complex, not hard-coded and are changeable by the end user. Preset default settings for maximum user privacy and security while allowing for the end user to change the settings. Develop IoT devices and software focused more on intended outcomes and meeting user needs and not for collecting data.

14. Establish periodic training programs for all personnel involved (employees, contractors, partners and third-party vendors) in the IoT ecosystem. The training shall include security (for laptops, mobile devices, beacons, endpoints, attached devices, static and portable storage, applications, ports, etc.), risk mitigation, laws and regulations, compliance, consumer privacy needs and overall IoT program strategy.

15. Meet the regulatory and compliance standards for all verticals that the IoT ecosystem is serving. For example, HIPAA for healthcare systems, and Sarbanes-Oxley compliance for the financial operations, PCI, DISA, etc. Identify the method and process to monitor, investigate and respond to compliance violations.

16. Develop IoT devices based on a nature of inclusion for a broad user base including people with disabilities, left and right-hand use, women's and men's proportions, underserved communities, etc.

Security

Build a system with security in mind from the start rather than including security in hindsight with consideration for the protection of public, integrity and resilience to attacks. Incorporate IT and OT security protocols and barriers to protect corporate data assets from intrusion. A system built with an ability for continuous adaptation to the new security risks and vulnerabilities allows for a better future-proofing of the IoT ecosystem.

1. Establish a governance committee that includes executive level representation and key stakeholders from various operational, strategic and service functions to provide IoT program direction and oversight.

2. Incorporate Managed Detection and Response (MDR) systems in addition to traditional firewall and malware security systems to proactively monitor, define and defend against intrusions.

3. Create a Security Operations Center to monitor and defend intrusions.

4. Establish a security framework that accounts for various levels of security risk and impact to a breach at an individual IoT ecosystem component level.

5. Safeguard the IoT ecosystem's data and other components by properly designating, establishing and securing access. Identify the various types and levels of access, including but not limited to: people, enterprise/agencies, systems, machines, software components, APIs, network etc. Establish procedures to monitor access and respond to access violations in an expedited manner. Regularly review and update access needs as components are added to or changed within the IoT ecosystems.

6. Provide training for employees. Most intrusions are due to employee errors.

IoT COUNCIL
POWERED BY ITA

7. Protect data at rest or data in motion, including the integrity of the data between intra and inter IoT ecosystem exchanges.

8. Establish a proper chain of custody of the IoT ecosystem and data. Simultaneously keep these systems maintained and monitored.

9. Develop a threat vulnerability and mitigation plan that includes responsibility assignments, threat thresholds, resolution steps, escalation procedures, and communication assignments. Upon identification and confirmation of a system breach, notify the affected parties and applicable regulatory entities in a timely manner and in compliance with applicable data breach notification laws.

10. Establish an audit-able ticket reporting, tracking and resolution system.

11. Monitor any IoT connected device throughout its complete lifecycle for security vulnerabilities and breaches. Distribute and install security patches for all IoT devices as soon as they are available, regardless of the formal support window for feature updates. The vulnerability of the system is as weak as the weakest component.

12. Take prompt action to identify the cause of the breach, identify the impact of the breach, correct the cause of the breach, and update threat mitigation planning to prevent repeat or similar occurrences. Whenever possible, consider a "defense-in-depth" strategy whereby multiple layers of security may be used to defend against a particular risk.

13. Be aware of common and known vulnerabilities and mitigation procedures to update IoT components accordingly in a timely manner. Regularly engage industry-recognized cyber threat information sharing platforms to learn and share information about new threats and resolution techniques.

14. Establish zero-day security breach services and defenses.

15. Regularly audit the IoT ecosystem, its affiliates and partners who impact the IoT ecosystem to identify vulnerabilities and create a plan of action to mitigate them. Test and apply security patches from third party entities as soon as they are available.

16. Ensure IoT devices and software are not distributed with known security vulnerabilities.

17. Seek appropriate law enforcement action and support if the law has been violated due to an unauthorized security access.

Data Management and Ownership

The IoT ecosystem must protect and respect rules of data management and ownership. The IoT system should be open and transparent about the ownership and retention of data, any transfers of data, and the chain of custody of data.

1. Be transparent about what data is collected, how data is processed, for what purposes data will be used, how data is retained, shared and disclosed, and whether data will be distributed to third parties. Define the purpose of collection, the time of collection and, at all times, limit the use of the data to the defined purpose. Give users choices about how their information will be utilized, mainly when the data collected is beyond the user's reasonable expectations.

2. Subject to applicable laws and regulations, the user owns the rights, title and interest in and to their own IoT data. Meanwhile, the

entity that collects, select, coordinates and/or arranges the data into a database or otherwise owns the rights, title and interest in and to the modifications it makes to the data.

3. If one party claims ownership of, or any rights in, the IoT data owned or generated by another party, this should be clearly stated in writing and consented to by the other party, such as, by way of example and not limitation, by means of an enforceable "click-wrap" agreement or a written agreement signed by the other party. During any transfer of ownership of the data, consider auditing the rules of sharing, transfer and retention of data.

4. Establish rights to access IoT data including, but not limited to, use, hosting, caching, storing, reproducing, copying, modifying, combining, analyzing, creating derivative works, communicating, transmitting, publishing, displaying and distributing IoT data. Allow the user access to data maintained about them, information on the source of the data, critical inputs into their profile, and any algorithms used to develop their profile. Enable individuals to correct and control their information.

5. If the entity/agency retains any license rights in data owned by a third party, the terms of the license should be readily available and clearly communicated to the third party.

6. Develop a Data Management Plan that includes, but is not limited to, data collection, analysis, access, preservation, categorization, dissemination, sharing, usage, derivation, verification, ownership, retention, security and disposal of data. The Data Management Plan needs to address internal and external entities along with their relationships and responsibilities to the potentially vast quantities of collected and derived data.

7. IoT data should be archived in a federated (centrally managed while locally available) way and made available throughout a catalog of documented open APIs unless restricted by existing policy, laws or regulations and/or doing so would compromise privacy.

8. Organizations should define protocols for industry data environments to ensure appropriate sharing of information.

9. Each IoT data set should be validated and verified and the resulting master copy clearly labeled before it is used, aggregated and/or released. Data should be versioned so that any updated data can be distinguished from the original and/or master copy. The retention and disposal policies for the master copy should be explicitly defined.

10. Establish, monitor and maintain data integrity, accuracy and validity for data at rest and in motion as the data is transferred between intra and inter IoT ecosystems.

11. Maintain proper chain of custody of the collected information and derived data.

12. Establish rules regarding the ownership of acquired data from either the combination of multi IoT ecosystems or from an IoT ecosystem and other external data sources.

13. Establish and manage policies for the transfer of the data to third parties, such as, by way of example and not limitation, vendors, interacting with the IoT ecosystem. Ensure that those third parties have comparable privacy and security policies as the entity that initially collected the data from the user.

14. Ensure any personal data collected is for a specific, explicit and legitimate purpose and not further processed, used or shared without appropriate anonymity processing on the data.

15. Conduct regular reviews to verify if results from profiling are responsible, fair, ethical and compatible with and proportionate to the aim for which the profiles are being used.

Privacy

The ubiquity of technologies has led to the exponential growth of consumer data from both digital and analog sources. While big data has tremendous potential, it also raises new and ongoing concerns about the nature of privacy and the means by which individual privacy might be compromised or protected.
IoT deployments must protect and respect the privacy of individuals and the confidentiality of the enterprise/agency. There is always a balance that needs to be established between transparency and access right.

1. IoT entities should respect and protect the privacy of those whose data they collect and comply with all applicable laws and regulations relating to privacy. These provisions include but are not limited to the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), Sarbanes-Oxley and the Gramm-Leach-Bliley Act (GLBA), PCI, DISA, EU's General Data Protection Regulation (GDPR), etc.

2. Establish proper data classification and rights to the data.

3. To the extent that an IoT entity collects private information, the entity should have a privacy policy disclosing how the data is collected, used, shared, published and otherwise treated. This privacy policy should be readily available for review.

4. Any personally identifiable information (PII) or confidential information that is collected and retained should be classified, at a minimum, as private or confidential. Additionally, the entity collecting and/or keeping such information should, at a minimum, use efforts which are reasonable for the type of information obtained to protect the data from unauthorized use or disclosure. What constitutes PII may be defined by applicable federal or state laws or regulations and may change over time; therefore, policies regarding PII, including the definition of PII, should regularly be reviewed.

5. Provide clear documentation of access to information, use of information, signing in to access information, transfer of data and chain of custody and control.

6. PII and confidential IoT data should have a delineated retention policy and secure disposal procedure.

7. PII and other sensitive IoT data should be stored and transmitted using suitable encryption, or, if not encrypted, PII should be anonymized before it is transferred or otherwise disclosed.

8. Enterprise/agency IoT data shall be maintained under the confidentiality and support needed to compete in the market.

9. Any established vendor to the IoT ecosystem will inherit the need for compliance with the privacy policy of the enterprise/agency. Ensure regular audit of this vendor is conducted to monitor compliance.

10. Apply data minimization principles to either collect no data, collect only less-sensitive data, anonymize the received data, retain the information for a brief period (create policies for data retention and storage) or collect just the necessary type or minimum amount of data as required by the IoT ecosystem components.

11. Include appropriate opt-out mechanisms regarding the collection of information that comply with applicable federal, state and local laws or regulations; or, if not required by applicable laws, and depending on the relevant industry or use of information, consider providing an opt-out mechanism. For example, policies will need to be

use-case specific, such as factory floor, public video monitoring, retail environments, etc.

12. Consider establishing a "right to be forgotten policy" for erasing the personal data promptly and when it satisfies the established "no longer required" requirements.

About the Midwest IoT Council

The Midwest IoT Council's mission is to drive the advancement of IoT technology, policy and industry, establishing Chicago and the Midwest as an epicenter of IoT. The Midwest is in a unique position to be a leader in the Internet of Things evolution. We have a rich history of supporting industries such as manufacturing, software, big data, retail and healthcare, giving the region the experience and knowledge to foster the development of the Internet of Things.
The Council is driven by the notion that we have all the pieces right here for the Midwest to emerge as a national leader in the advancement of the Internet of Things.

About the Authors

The Policy Committee of the Midwest IoT Council includes:

Co-Chairs

- Andrew Goldstein, Partner, Freeborn & Peters LLP
- Mrinalini Lakshminarayananan, Sr. Director Product Management, Gogo

Committee Members

- Ziad Azzi
- Brenna Berman, Executive Director, City Tech Collaborative
- May Chan, Enterprise Solutions Architect, Vizions In Motion
- Rajesh Char, Director, Digital Customer Experience, RICOH
- Michael Donahue
- Abraham Emmanuel, Deputy Commissioner for Traffic Safety and Technology, City of Chicago, Department of Transportation
- Mark Handy, Principal, KenJiva Energy Systems
- Karthik Kandamuri
- Henry Kelly, Partner, Kelley Drye & Warren LLP
- Joleen Kuchenbacker, Senior Manager, Global and NALA Services Delivery PMO, Zebra
- Prem Lalvani, Director of Finance, Engine GRP
- Annette Memishofski, Aptitive
- Adam Sobol, CEO/Founder, CareBand
- Kelley Sommerfeld, Senior Manager, United
- Paul Steinberg, CTO, Motorola
- Dan Stibolt, Alliances Manager, Hitachi
- Jim Weatherhead

IoT Council Champions

Thank you to our IoT Council Champions. These organizations have invested in the mission of the Council and are helping to drive the IoT ecosystem of the Midwest forward.

Reference

• NY IoT Guidelines - https://iot.cityofnewyork.us/
• Mobile Marketing - https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/mobile-marketing/
• Collection, Use, and Maintenance of Marketing Data - https://thedma.org/accountability/ethics-and-compliance/dma-ethical-guidelines/collection-use-and-maintenance-of-marketing-data/
• White House (Obama) Report on Big Data and Privacy - https://obamawhitehouse.archives.gov/blog/2014/05/01/pcast-releases-report-big-data-and-privacy
• EU's IoT Governance, Privacy and Security Issues - http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Governance_Privacy_Security_Final.pdf
• EU General Data Protection Regulation (GDPR) - http://www.eugdpr.org/; https://gdpr-info.eu/
• ITIF's review of China's ICT Innovation Policy - http://www2.itif.org/2014-china-ict.pdf
• India's vision for its IoT plan (Draft IoT Policy) - https://www.intel.com/content/www/us/en/policy/policy-internet-of-things-iot.html
• United Nations (Global Pulse) Recap on Int'l Conference of Data Protection & Privacy Commissioners - http://www.unglobalpulse.org/International-Conf-Data-Protection-Privacy-Commissioners2014-Recap
• US Federal Trade Commission (FTC) Report on IoT Privacy & Security - https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
• US Federal Communications Commission (FCC) Privacy Act Information - https://www.fcc.gov/general/privacy-act-information
• Internet of Things Cybersecurity Improvement Act of 2017 (US Senate Bill) - https://www.warner.senate.gov/public/index.cfm/2017/8/enators-introduce-bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-iot-devices; https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017
• US Dept. of Commerce (DOC) Internet Policy Task Force and Digital Economy Leadership Team's Green Paper on FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS - https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf
• US Children's Online Privacy Protection Act (COPPA) - http://www.coppa.org/coppa.htm
• Intel's IoT Public Policies - https://www.intel.com/content/www/us/en/policy/policy-internet-of-things-iot.html
• Array of Things Governance & Privacy Policies - https://arrayofthings.github.io/final-policies.html