Back to the Future in Device Security

Leveraging FIPPs to Proactively Manage IoT Privacy and Security Risk

Doron Rotman, CIPP, is a managing director at KPMG LLP, the US national privacy service leader for KPMG and a member of KPMG international privacy leadership team. He has more than 30 years of experience, focused on providing privacy, security and information governance services.

Chris Kypreos, CIPP, is a senior associate at KPMG LLP, and a member of the International Association of Privacy Professionals (IAPP). Kypreos has helped develop and author several publications and has presented at industry events.

Sarah Pipes, CIPP, is a senior associate at KPMG LLP, and is currently on rotation at KPMG Belgium. Pipes is a member of the IAPP. She has helped develop and author several publications and spoken at several industry events.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and choose the Comments tab to share your thoughts.

Go directly to the article:

The Internet of Things (IoT) represents an unknown set of forces. However, one known is that IoT-connected devices will generate exponential levels of new data that will lead to powerful insights, drive new business and facilitate the development of innovative technologies. IoT also raises multiple data privacy and security concerns when new data sources combine with legacy sources to reveal new insights about individuals through predictive analytics that may be inconsistent with the original purposes for collection and use. Additionally, connecting new technologies with legacy systems can prove risky, as many new IoT device manufacturers lack software development and security experience.[1] These risk factors can increase a company's threat exposure and make the organization a ripe target for a breach.

Despite IoT's unknowns and the corresponding privacy and security risk, there are legacy tools available that privacy and security leaders can use to address these risk factors proactively. This article shows how frameworks based on the Fair Information Practice Principles (FIPPs)[2] are adaptable and practical tools to help embed privacy and security into new IoT devices.

EVALUATING PRIVACY AND SECURITY: A FRAMEWORK

Although IoT represents a state of change and advancement, a common set of principles can serve as the foundation for companies seeking to understand and manage privacy and security early in the design and development phases of new connected devices. One set of principles is FIPPs, which the US Department of Health, Education, and Welfare referenced in a 1973 report. The Organisation for Economic Co-operation and Development (OECD) revised the principles in 1980. Today, FIPPs serves as the basis for multiple codified privacy laws, regulations and standards throughout the world.[3]

Auch auf Deutsch verfügbar
www.isaca.org/currentissue

FIPPs-based standards continue to be useful for privacy and security professionals to evaluate and design their IoT programs and technologies because they are actionable and comprised of risk-based controls, and they are adaptable to the unique characteristics of a particular industry and an organization's business requirements.

Two FIPPs-based frameworks available are the Generally Accepted Privacy Principles (GAPP)[4] and the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.[5]

FRAMEWORK 1: GAPP

The GAPP framework was developed by a taskforce formed by the American Institute of Certified Public Accountants (AICPA) and CPA Canada. Its primary purpose is to assist management in creating an effective privacy program that addresses privacy obligations, risk and business opportunities. Therefore, the 10 principles and 73 control criteria within GAPP are designed to assist with the implementation and demonstration of better privacy practices. The framework additionally includes a maturity model that organizations can use to assess their overall maturity.

The 10 GAPP are:

1. **Management**—The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice**—The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.

3. **Choice and consent**—The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. **Collection**—The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention and disposal**—The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulation and thereafter appropriately disposes of such information.
6. **Access**—The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties**—The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy**—The entity protects personal information against unauthorized access (both physical and logical).
9. **Quality**—The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement**—The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

These principles address not only strong privacy practices, but their implementation by the organization.

FRAMEWORK 2: NIST SP 800-53 APPENDIX J

NIST commissioned a Joint Task Force Transformation Initiative to publish SP 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations," which provides a catalog of security controls designed to support the security control selection for US federal information systems. Within this larger standard, the Appendix J Privacy Control Catalog was developed to provide a road map for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of personally identifiable information

(PII), whether in paper or electronic form.[6] These controls are designed for use by chief privacy officers (CPOs) to support their organizations in complying with privacy components of applicable federal laws and other requirements. This is achieved in part through simplifying requirements into a single catalog through mapping overlapping controls found in various privacy and security requirements.

To achieve this, appendix J includes a structured set of controls across eight control families. These privacy control families are:

1. **Authority and Purpose**—This family ensures that organizations:
   - Identify the legal bases that authorize a particular PII collection or activity that impacts privacy
   - Specify in their notices the purpose(s) for which PII is collected
2. **Accountability, Audit and Risk Management**—This family enhances public confidence through effective controls for governance, monitoring, risk management and assessment to demonstrate that organizations are complying with applicable privacy protection requirements and minimizing overall privacy risk.
3. **Data Quality and Integrity**—This family enhances public confidence that any PII collected and maintained by organizations is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in public notices.
4. **Data Minimization and Retention**—This family helps organizations implement the data minimization and retention requirements to collect, use and retain only PII that is relevant and necessary for the purpose for which it was originally

collected. Organizations retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a US National Archives and Records Administration (NARA)-approved record retention schedule.

5. **Individual Participation and Redress**—This family addresses the need to make individuals active participants in the decision-making process regarding the collection and use of their PII. By providing individuals with access to PII and the ability to have their PII corrected or amended, as appropriate, the controls in this family enhance public confidence in organizational decisions made based on the PII.
6. **Security**—This family supplements the security controls in appendix F to ensure that technical, physical and administrative safeguards are in place to protect PII collected or maintained by organizations against loss, unauthorized access or disclosure, and to ensure that planning and responses to privacy incidents comply with OMB policies and guidance. The controls in this family are implemented in coordination with information security personnel and in accordance with the existing NIST Risk Management Framework.
7. **Transparency**—This family ensures that organizations provide public notice of their information practices and the privacy impact of their programs and activities.
8. **Use Limitation**—This family ensures that organizations only use PII either as specified in their public notices, in a manner compatible with those specified purposes or as otherwise permitted by law. Implementation of the controls in this family will ensure that the scope of PII use is limited accordingly.

GAPP and NIST SP 800-53 appendix J can trace their origins to FIPPs, and their flexibility and comprehensiveness have made them the predominant standards to evaluate privacy and security. Both standards are customizable, and organizations can leverage them to implement new organizational processes or as guidance to embed privacy and security controls into new IoT products and systems. Both are designed for management use and facilitate the implementation of privacy requirements rather than simply stating the end goal.

However, each framework also has unique strengths. NIST SP 800-53 appendix J is designed to facilitate compliance with numerous overlapping US federal laws, directives and orders, and, therefore, it is a legally driven framework. While appendix J is a useful tool for organizations across many industries, the primary audiences are those required to satisfy US federal requirements. Therefore, it is most useful for implementing IoT technologies in industries that must comply specifically with US law. Conversely, GAPP does not support compliance with any particular law, but rather international good practices. It is most useful for IoT technologies that will be implemented in a similar way internationally, with modest modifications to meet local requirements.

The two case studies that follow illustrate the effectiveness of the principles contained within each framework in designing cutting-edge IoT products.

USE CASE 1: SMART CAR—GAPP

The automotive industry views connected cars as the way of the future. The connected vehicle will incorporate technologies that enhance human safety, reduce traffic congestion, improve efficiency and vehicle performance, and provide valuable information services.[7] Moreover, analysts predict that the global market for connected vehicles will reach 220 million cars on the road by 2020.[8]

Although nearly all major automobile manufacturers and communication companies have entered the connected car market, evidence demonstrates that many companies continue to develop products with key privacy and security vulnerabilities. US Senator Ed Markey commissioned a report based on the responses of 16 major manufacturers that revealed a clear lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle or against those who may wish to collect and use personal driver information.[9]

Auto companies have demonstrated a commitment to privacy, and the Alliance of Automobile Manufacturers Inc. and Association of Global Automakers developed a self-regulatory framework, Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technology Services, to address these concerns. Each participating member will commit to compliance with the principles for new vehicles manufactured no later than model year 2017.[10] Although the principles provide guidance to members on how to satisfy the requirements, privacy leaders can leverage the GAPP framework's controls to support their compliance efforts and address future privacy and security risk in the planning and design phases.

Case Study Background

An auto manufacturer (the company) plans to develop software that they will install on their vehicles' built-in navigation system. The application will integrate via Bluetooth to an individual's mobile device to sync the user's contact addresses with the car's navigation system. The company can leverage the GAPP framework in the process of designing, developing and installing the application.

GAPP Management Principle

The company should assign a privacy product manager who will be an accountable party and will perform a privacy impact assessment at the project's outset to identify the associated risk based on the personal information collected, stored and transferred. The privacy manager will interact with various departments, including software development, legal and product supports, to understand business and regulatory requirements and monitor new obligations posed by changes in the business and legal environments.

GAPP Notice Principle

The company understands that notice is a foundational element in privacy laws and standards. The team is also aware that providing notice in the context of connected devices can be difficult when user interfaces are often nonexistent or limited. However, notice does become essential when data use is inconsistent with user expectations and in the cases of new purposes. The company can provide notice when a customer initially registers to use the application or identify alternate mechanisms to provide notice, including a web site that includes links to demonstrations and tutorials of the software's functionality.

GAPP Choice and Consent Principle

The company's software is functional because it integrates certain personal data elements with geo-location data. Similar to notice, the privacy manager understands the challenges in providing knowledgeable opt-in consent over limited interfaces. The company should consider providing various tiers of service to customers based on the level of consent provided. For example, drivers may elect to share the vehicle's current location with other members of their network to provide two-way visibility. Alternatively, the customer may prefer to consent only to the use of static address data entered into the device. By understanding the various use cases for the software, the company can offer granular choices that limit personal information usage without affecting functionality.

GAPP Collection Principle

The company understands that data collection becomes more critical in the IoT context, where most networked devices consistently collect and process data. Combining large data sets can offer powerful knowledge and analysis, but data usage may be inconsistent with the primary purposes of collection. The company should limit data collection to lawful methods and be transparent with customers as to how it collects and integrates personal information from third parties. Additionally, the company can reduce its potential risk for breach and associated liability by limiting data collection to only those elements that are essential for functionality. By incorporating data minimization controls into the application, the risk associated with notice, consent and retention becomes less magnified.

GAPP Use, Retention and Disposal Principle

The integration of the company's software with other devices and programs may enhance the customer experience, but the company should limit the use of data to primary business purposes or cases where the customer provided explicit consent. Additionally, the privacy manager should consult other stakeholders in the organization on business and legal retention requirements to enable those departments to create record-retention schedules. Then, the privacy manager should implement procedures to ensure the destruction of data upon expiration of record-retention dates. For example, the company could consider deleting all data stored by the software at the conclusion of each driving session and then reinitiate the connection when the driver starts the vehicle the next time. This will help reduce the risk of a data breach and can improve program functionality. The company should perform regular audits to test compliance with policies and procedures.

GAPP Access Principle

The company should recognize that allowing customers to access and update their data will result in a positive-sum experience. This improves accuracy and relevance of the data presented through the software to the customer. If the company

elects to store customer data, it may offer a secure web portal that customers can access to easily update and delete their information. By leveraging alternate technology, the company can work around limitations presented by IoT devices.

GAPP Disclosure to Third Parties Principle
The company may determine that the functionality of the software increases if there is integration with other third-party providers. By using GAPP, the company will better understand how to protect its customer information. The company will recognize that any new purposes for the data should require customer consent. Additionally, the privacy manager can work with legal counsel to ensure that appropriate provisions are included in third-party contracts based on the services provided.

GAPP Security for Privacy Principle
The company must understand the importance of application security in the design phase to protect customer data throughout the collection, storage and transfer phases of the life cycle. The privacy manager should work with the information security team to embed controls into the supporting IT infrastructure. The company should consider data encryption, both at rest and in transit, when information transmits from the device to the vehicle and from the vehicle to other third-party providers involved in the process. Additionally, the company can deploy industry-level access management solutions that limit access to personal information to only authorized and authenticated individuals.

GAPP Quality Principle
The company provides a service to its customers that relies on offering real-time data that are accurate and relevant. It is critical for the data collected to be normalized and consistent with the original entry status. Although the customer initially enters contact information into the mobile device, the company can ensure data quality by leveraging uniform protocols and controls.

GAPP Monitoring and Enforcement Principle
The company recognizes that good customer service requires offering mechanisms for the customer to engage the business. Although not unique to IoT, the company can establish a process to receive and respond to privacy and security inquiries and complaints. Additionally, the privacy manager should be responsible for ongoing monitoring of the environment for compliance and new business risk.

How to Apply GAPP
Most of these principles are applicable for IoT device manufacturers or software developers embedding privacy and security into the development process. However, GAPP facilitates flexibility: if specific principles, or even criteria within a principle, are not applicable to a particular development scenario, these can be documented and scoped out of the privacy assessment.

> "GAPP facilitates flexibility."

There is also flexibility in measuring of success in meeting the requirements laid forth by the GAPP principles. The AICPA and CPA Canada suggest the use of a Privacy Maturity Model based on the Capability Maturity Model (CMM). This model includes the following five levels: *ad hoc*, defined, repeatable, managed and optimized. The appropriate or desired state is determined by the organization, with acknowledgement that the highest level of maturity (optimized) may not be suitable for all or even many situations.

GAPP is a tool developed to help management create a practical and effective privacy program, and the 10 principles build to create a comprehensive management framework, addressing risk while enabling companies to retain their competitive advantage.

USE CASE 2: CONNECTED MEDICAL DEVICES—NIST SP 800-53

The connected medical device market is increasing rapidly, and analyst research predicts that the global remote patient monitoring devices market will grow to nearly US $1 billion by 2020.[11] As the number of wearable devices and monitoring technologies increases, concerns around the collection and storage of sensitive patient data will also continue to rise. As a result, the health care industry continues to be a vulnerable and attractive target for cyberattacks. In fact, recent research predicts that the health care field could face as much as US $5.6 billion annually in costs associated with data breaches.[12] US health care providers are subject to specific privacy and security requirements in accordance with the US Health Insurance Portability and Accountability Act

(HIPAA); therefore, it becomes critical that organizations safeguard their data and information systems to control access to systems, reduce privacy and security risk, and ensure data quality.[13] An organization can proactively leverage NIST SP 800-53 appendix J to help meet its compliance requirements under HIPAA and when evaluating new information management systems and other connected devices to ensure inclusion of appropriate privacy and security controls.

The following controls reflect the need to protect privacy throughout the information life cycle, from data collection to processing and maintenance through data sharing and destruction. The risk associated with each control area, therefore, is determined by the nature and processing of the personal data in question.

Case Study Background

In an effort to lower health care delivery costs and improve delivery quality, a veterans' affairs health care system (the organization) seeks to upgrade its health care information management (HIM) system to manage the exponential increase in data received from IoT medical devices. For example, at-home health monitoring devices provide transmissions of vital signs such as blood pressure and heart rate and can also measure symptoms related to diabetes, hypertension and asthma, among other diseases. Wearable devices can trigger an emergency response when necessary, while fitness bands provide information about exercise (e.g., steps taken, calories burned) throughout the day. The health care system's technology staff understands that there are various privacy and security requirements and prefers to scope mitigating controls during the planning and development phases.

Authority to Collect

The organization relies on collecting sensitive data elements to deliver quality and timely care to its patients. While reviewing the requirements relating to gathering information for the new HIM system, the technology staff should perform a privacy risk assessment to identify the risk associated with the collection of certain data and document the categories of elements in the privacy notice delivered to patients.

Accountability, Audit and Risk Management

The organization designates a privacy official to perform a privacy impact and risk assessment to identify the risk to personal information when deploying a new HIM system in the environment. This official and the technology staff understand that they should design systems with automated privacy controls that mitigate risk and reduce the likelihood of a breach. This step is critical, because the cost of redesigning privacy and security into the system after the fact is overly burdensome and expensive. By designing automated controls into the system, the organization understands that it can more effectively satisfy its monitoring and reporting requirements while increasing data security.

Data Quality and Integrity

The organization understands that maintaining accurate data in the health care context can be a matter of life and death. Doctors, nurses and medical professionals working with outdated data risk prescribing the wrong medications, which can potentially kill a patient. The privacy official should evaluate controls designed to ensure accuracy and validity of data upon entry into the HIM. Additionally, ensuring data quality becomes more critical as the system integrates with various connected devices storing and transmitting data in different formats.

> "Ensuring data quality becomes more critical as the system integrates with various connected devices."

Data Minimization and Retention

Although health care organizations have business justifications to collect most types of sensitive data, the organization understands it can reduce the risk of a breach by limiting collection of data to only that which is necessary and destroying sensitive data records upon expiration of the retention requirements. Additionally, the privacy official can coordinate with various departments to identify specific business requirements for extended data retention. Although the organization may retain certain data for testing purposes, the privacy official can explore de-identification and aggregation techniques to reduce privacy and security risk.

The organization's technology staff can help design controls to flag sensitive data elements and mask patient records to better support the data minimization and records disposal processes.

Individual Participation and Redress

Although health care providers can share protected health information (PHI) with limited restrictions for treatment, payment and operations reasons, the organization understands that patient consent and access are fundamental concepts in the decision-making process.[14] The organization builds trust with its patients when it provides them control over their information and allows them to update records to help improve data quality and accuracy. The privacy official should ensure that customer portals and other connected devices interfacing with the HIM provide access and certain control over the data records.

Security

To effectively secure personal information throughout the data life cycle, it is imperative that the organization document the various data flows. While designing the new HIM system, the privacy official should identify the different upstream and downstream systems and applications, the data elements contained in those systems, and the different data elements transferred from one system to another. Then, the privacy official can work with the organization's information security team to ensure that the different systems in the inventory receive the appropriate level of security based on the sensitivity of the data.

Transparency

The organization collects data from the connected devices that integrate with the HIM system. Therefore, the organization should provide notice to its patients on the types of information collected, processed, stored and transferred through these connected devices. If the wearable technology has limited interfaces, the privacy official should consider alternate methods to provide notice with these devices. For example, the organization may consider publishing its privacy notice on a web portal where patients access and input personal information.

Use Limitation

The organization understands the importance of patient trust in the doctor-patient relationship. The privacy official should incorporate controls and checks that limit the opportunity to access and use information for new and secondary purposes not accompanied by customer consent. However, HIPAA permits the sharing of certain records with other covered entities and business associates, incorporating audit log capabilities within the HIM system to help track data transactions to assist with the ongoing monitoring of data sharing and user access.

How to Apply Appendix J

This standard is designed to support effective compliance within the scope of privacy requirements by supporting compliance throughout the information governance cycle. While NIST SP 800-53 appendix J does not incorporate all US laws, especially those guiding particular data types such as health information, these additional laws can be incorporated easily at the appropriate stages of the existing framework. Appropriate compliance with controls also depends upon any additional requirements that may apply, and the organization may choose to implement optional "control enhancements" where there is a demonstrated need.

> "To address these issues and challenges, companies must incorporate privacy and security from the outset when looking to adopt, design and deploy new connected technologies."

NIST SP 800-53 appendix J is applicable to various use cases to assist in the build out of the organization's privacy program. The privacy official can leverage the control framework when establishing an overarching program governance structure and when seeking to deploy new IoT systems and applications in the environment. The organization can customize the controls based on operational needs, but it provides a series of guidelines to embed privacy into the environment.

CONCLUSION

IoT represents great and unpredictable change in the way data are collected, processed, stored and analyzed. New technologies will significantly improve the way companies operate their business and interact with customers and other organizations. In this sense, IoT symbolizes great promise, but it also poses risk to personal privacy and security, including

collecting and processing data for new purposes beyond their original intent and generating amplified risk associated with insecure devices and target-rich data sources. To address these issues and challenges, companies must incorporate privacy and security from the outset when looking to adopt, design and deploy new connected technologies.

FIPPs represent the foundational elements of many comprehensive risk- and control-based privacy frameworks. Organizations can leverage FIPPs-based frameworks, including GAPP and NIST SP 800-53 appendix J, to evaluate the privacy and security issues posed by new IoT devices, help their organizations design and integrate secure technologies, and reduce their overall risk levels. Although IoT is changing the way data are collected, processed and used, FIPPs contain relevant guidelines for companies to manage privacy and security proactively in the design of new IoT devices.

ENDNOTES

[1] *The Economist*, "Their Own Devices," 18 July 2015, *www.economist.com/news/science-and-technology/21657766-nascent-internet-things-security-last-thing-peoples*

[2] Department of Health, Education and Welfare, *Records Computers and the Rights of Citizens*, USA, July 1973

[3] Gellman, R., "Fair Information Practices: A Basic History," 31 December 2008, *http://bobgellman.com/rg-docs/rg-FIPShistory.pdf*

[4] American Institute of Certified Public Accountants and CPA Canada, "Generally Accepted Privacy Principles," March 2011, *www.aicpa.org/INTERESTAREAS/INFORMATIONTECHNOLOGY/RESOURCES/PRIVACY/GENERALLYACCEPTEDPRIVACYPRINCIPLES/Pages/default.aspx*

[5] National Institute of Standards and Technology, Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, USA, 30 April 2013, Appendix J

[6] *Ibid.*, p. J-1

[7] Auto Alliance, "Auto Issues—Automakers Believe that Strong Consumer Data Privacy Protections are Essential to Maintaining the Trust of Our Customers," 13 November 2014, *www.autoalliance.org/index.cfm?objectid=46DD7290-68FD-11E4-866D000C296BA163*

[8] Greenough, J.; "The 'Connected Car' Is Creating a Massive New Business Opportunity for Auto, Tech, and Telecom Companies," *Business Insider*, 19 February 2015, *www.businessinsider.com/connected-car-statistics-manufacturers-2015-2*. Note that the definition of "connected cars" used in this study is: "built with the necessary hardware to connect to the Internet."

[9] Markey, E., "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk," February 2015, *www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf*

[10] *Op cit*, Auto Alliance

[11] Transparency Market Research, "Remote Patient Monitoring Devices Market—Global Industry Analysis, Size, Share, Growth, Trends and Forecast, 2014–2020," June 2015, *www.pharmiweb.com/pressreleases/pressrel.asp?ROW_ID=117619#.VahJ0vlVgli#ixzz3g6TRMnS2*

[12] Ponemon Institute, "Fourth Annual Benchmark Study on Patient Privacy & Data Security," 12 March 2014, *www.ponemon.org/blog/fourth-annual-benchmark-study-on-patient-privacy-and-data-security*

[13] Congress, Health Insurance Portability and Accountability Act of 1996, (Pub. L. 104–191), USA, 21 August 1996

[14] Department of Health and Human Services, "Uses and Disclosures for Treatment, Payment, and Health Care Operations," 45 CFR 164.506, USA, 3 April 2003, *www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/sharingfortpo.pdf*