Chapter 4

Security and Privacy for Location Services and the Internet of Things

In the previous three chapters of this issue of *Library Technology Reports*, topics covered include a Bluetooth low energy (BLE) beacon Internet of Things (IoT) implementation that enabled location-based recommendation services in library book stacks; integrating recommendations of electronic content using print content as a reference point for those recommendations (chapter 2); and the range of technologies (from RFID to NFC and modular mobile devices) that make the IoT possible, along with value-added location services (chapter 3). Now that we understand IoT through the lens of a case study and through the exploration of IoT technologies enabling connected environments, the topic of security should be explored in depth. As we have seen, these technologies are not without ethical and legal ramifications.

For this final chapter, we explore security and privacy for location services and IoT. Within IoT technologies, several important security and privacy implications have surfaced. In this chapter, we will unpack and lay out in detail the specific ethical considerations that need to be addressed. The security and privacy implications include the need for specific privacy policies that govern IoT location services in libraries and other academic settings in general. Especially concerning are the possibilities that will exist for mass surveillance on a scale larger and more profound than what was possible in the web environment. We have also seen from the previous chapters that there are unique IoT security considerations for location services in libraries that stem from the decentralized nature of IoT technology. It is with these problems of decentralization and location-based solutions in mind that an in-depth treatment on the types of general privacy and security among the IoT is required. After exploring general privacy and security considerations of IoT technology, we delve into the specific considerations of applied location services within the IoT.

In *Designing Connected Products: UX for the Consumer Internet of Things,* the authors defined general computer security as "the degree to which a system can protect the assets it contains from unauthorized access, modification, or destruction."[1] This is the classic paradigm used in a number of systems previous to the onset of IoT system design. Note, however, that within the IoT, "Connecting up the physical world creates the potential for malicious hacking to have 'real world' consequences."[2] The authors went on to note several of the physical world implications of an IoT environment, including the possibility for automobile hacking and compromising unsecured networked cameras. Compromising automobile security can have dire consequences for those who are beginning to rely on automated systems. Some hackers may do this purely to provide amusement and may not be out to cause any kind of maliciousness, while yet other hackers are interested in causing harm as a result of their IoT hacking. For every positive and life-changing part of the IoT that stands to improve quality of life and services in general, there comes with a corresponding security risk. If security is compromised, then the possibility is high for the privacy of the users to be compromised as well. The significance of security to privacy is high since in general the IoT encompasses many networked computing resources exchanging data. The IoT relates to privacy: "if security is a network issue, privacy is a networked data issue."[3] One of the leading overarching issues that system designers are still struggling with answering both for commercial application and within the IoT for location services in libraries is the extent to which privacy can be realistically assured, given the new velocity at which data are generated and shared.

General Privacy Considerations within Libraries

What are the set of concerns that we are focused upon when we talk about privacy in the IoT? To what extent can we expect even general privacy in the current era of online access? In our current digital era of always on, always connected environments, many of the newer advances of networked systems have challenged our traditional notions of privacy. Like the IoT trend, the trend within higher education to focus on personal learning analytics has also pushed the boundaries of privacy for students. In at least one study from the University of Minnesota, personally identifiable data are utilized in order to generate correlations among student success by first-year students and library use.[4] Learning analytics stems from the need to make real-time decisions about students that impact advising and course work. The level of detail and monitoring of students that learning analytics delves into is akin to collecting data at most touch points within the online learning ecosystem of a university—all logins to computer systems are logged and analyzed for data points. It is theorized that data points collected could be the basis for an intervention by a professor, an advisor, writing tutors, or librarians.

It is likely that IoT data will eventually help support data generation for learning analytics as possible data points that could inform potential interventions of academic assistance to students. Therefore, it is through a learning analytics lens that we can approximate several potential IoT privacy implications.

Within those conversations about learning analytics, librarians have focused on several documents to help navigate choices about student privacy. These documents include local patron privacy documents—for example, what are the existing policies in place that govern circulation records? These documents are usually grounded by the American Library Association (ALA) principles, which include an interpretation of privacy as it relates to the Library Bill of Rights. The ALA's privacy statement notes that "Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The ALA has affirmed a right to privacy since 1939."[5] With regard to the privacy implications inherent within IoT, since system designers and technologists are now able to locate users when guiding them to the location of items in book stacks, we should reference these intellectual foundations as we seek to provide services that support the mission of libraries—to provide access to information. What is troubling to note, however, relates to the decentralized nature of the IoT and the fact that multiple third-party tools and technologies may come into play within the context of the IoT.

As Weinberg and others noted in their article "Internet of Things: Convenience vs. Privacy and Secrecy," "Consumers can interact with IoT devices, but in many cases they don't directly enter the data. Rather IoT devices by themselves monitor and retrieve relevant data from the environment and a person."[6] They went on to note that, "In an IoT environment, data are shared with providers and with other devices,"[7] which places the library in a troubling area for maintaining privacy. As users begin to interact with IoT-type services, they may not even be aware that data are collected and retained. Because they do not know beforehand, these same users would not think to consult a privacy policy for the service. Libraries may not be able to govern what happens when those library services are built upon IoT devices that share data with other devices. However, libraries making use of IoT technologies should make privacy policies easy to find and access by users of a service before they make use of the IoT service. Therefore, new policies that speak to how IoT infrastructure interacts with user data are needed, along with an overt and proactive recognition about when data are sent to third parties and how third parties stand to use such data. In general, privacy policies within the IoT should include assigning responsibilities of data privacy through each portion of the "data pipeline" through any service, whether it be a database, sensor data, or an application: "Service providers need to identify carefully roles and responsibilities in the processing of personal data by everyone involved in providing a service and the equipment to support it so that liabilities are well understood" and "any data—even if it originates from 'things'—can be considered personal data if it is able to reveal information about the personal life of individuals."[8]

Several additional possibilities in designing for general privacy within IoT include

- Not storing data in third-party systems.[9] Have user data remain only with the user. This principle takes some of the advantages of decentralized systems of which the IoT is comprised and uses that for data persistence within the user's devices or peripherals. If the data always stay with the users, then the user can better take control over how their personal data may be utilized.
- If data are retained, delete the data after a set amount of time.[10] This would help ensure that users of the system from years ago do not have to worry about a data breach in five years. I would recommend that your library system delete user data after one year.
- Privacy policies should be made public and shared specifically with users of an IoT service. If third-party systems end up with user data, it would

> behoove the organization providing that access to understand how those data are used and how long users can expect their data to be retained.

Privacy becomes a more heightened and sensitive area when dealing with multiple data points and service providers.

Security for the Internet of Things

The current state of security for IoT is troubling since IoT technology suffers from its relative newness. The security of IoT is simply untested for service delivery. As an example, Cricket Liu, a chief infrastructure officer, wrote in "Securing Networks in the Internet of Things Era" that "most connected devices don't support strong authentication mechanisms such as 802.1X, leaving network administrators to use their mac addresses—or nothing—as a weak form of authentication."[11] What this means is that not only is current state-of-the-art security not used for IoT technologies, but that degraded security is currently the best that can be offered for some services and products. This is concerning indeed, given that the IoT encompasses smart objects used in the home and throughout the physical world—like cars or monitoring systems like networked cameras and the like. Another problem to consider in the IoT is the number of devices and technologies. Weinberg and others noted that, "With the proliferation of technology and the associated growth in data and databases, the opportunity for compromise can increase and the effects can be great."[12] The database, as a mature technology, does have some foundational and well-understood security best practices when those databases exist in servers.

Database security in library settings has long been a concern when protecting web-based services. In the wake of recent government-sponsored surveillance that was uncovered with the Snowden revelations, the security of databases and the personal use data that libraries steward has seen a renewed interest. In a recent issue of *Library Technology Reports* on privacy and security for library systems, several scenarios of web-based services are considered: "Transmission of patron sessions over the Internet evokes similar issues and requires proactive measures to maintain consistency with library privacy policies. To protect privacy organizations need to consider the protection of both 'data in motion' as it traverses networks and 'data at rest' as it is stored on servers."[13] These distinctions are also applicable to IoT security since there are vast amounts of data that reside, are transmitted, and then are stored finally as server data. In some cases, this server data will collect logs and logs of data unless programs are put in place to expunge these records. It should be noted that by default, few professionals ever know about the logging that their own machines are preconfigured to do. Even fewer will consider that this problem is further complicated by the fact that third-party logging may be out of the domain of library professionals. This is nowhere more evident than the case of third-party databases, like journal providers that collect data on usage that are generated by users and then sold or otherwise monetized. When users create accounts in the third-party tools, the situation becomes even more egregious, since a personal profile of a user may now be able to be constructed by parties outside control of the library. Therefore, library professionals ought to ask third-party vendors what data are collected about the library users and inquire how any third-party data collected will remain secure.

With regard to the security of personal data within the IoT environment, almost all data that travel wirelessly (e.g., Wi-Fi, Bluetooth, and NFC, to name several we have considered in this work) hold the potential of being grabbed by a third party through interception unless they are encrypted to a degree that is an industry standard. As a rule, all IoT wireless data should aim for strong end-to-end encryption. Liu noted several additional planning solutions in securing the IoT: "To prevent network teams from becoming overwhelmed as greater numbers of more varied devices join the IoT, consideration should also be given to network control and automation systems, which can help tackle the inevitable increase in time-consuming manual tasks such as IP address management which are caused by an exponential increase in the number of devices on the network."[14] At a more technical level, consider that requirements for security should include "support for 802.1X, DHCP, SNMP management, remote upgradeability and IPv6."[15] These are several mature technology enhancements that should be asked of IoT vendors by IT leaders in the future when considering adapting services for libraries and academic settings.

Securing Internet of Things Hardware

The IoT is inherently about bringing connectivity to every part of the physical world. With regard to the physical tangibility of IoT technology, hardware designers will need to "take steps to make them less likely to be stolen or physically accessed by unauthorized parties, such as designing product housings to prevent tampering or make it apparent when the device has been tampered with."[16] In the Estimote example from the second chapter of this work, we have a type of technology that is fully encased, and tampering is less likely with a product with enclosed shells. It was also the case that with the Estimote case study, the beacons themselves were hidden from view of the users of the building. This makes it even less likely that some devices could be compromised by someone accessing their physical components. The physical components that might make an Estimote beacon a target include its battery—which may have value in and of itself. Removing even one Estimote from an array of beacons in the library may result in service degradation—and if enough are missing from a specific section, it could result in system failure as well.

In applying these considerations to the general security of IoT hardware, consider that third-party tools like sensors or beacons should be purchased in such a way that tampering would not be possible. Avoiding those problems early in the deployment process should be paramount, since starting an IoT service with insecure devices is not a good way to develop buy-in or support from people using the service. Furthermore, several devices may come with firmware updates so that the hardware could be updated with security patches before the system is deployed.

Securing Internet of Things Middleware

Middleware in the IoT is a component that helps to manage and provide data and business logic to smart, connected hardware. According to the work "A Security Survey of Middleware for the Internet of Things," "Middleware has been defined as computer software that has an intermediary function between the various applications of a computer and its operating system."[17] Middleware will be increasingly required for the IoT to function since it will be difficult to manage and administer the growing expansion of connected devices. Traditional automation tells us that some level of middleware can help support and streamline management of devices. Enterprise software in the IoT will almost always be middleware-driven. A review of IoT middleware security explored the use of a Web Services model for security, with Fremantle and Scott finding that traditional SOAP/Web Services models of security present challenges in "performance, memory footprint, processor power and usability," since these are constrained resources within the IoT.[18] The Web Services model is also generally for objects that are stateless, which is harder to ensure in the IoT, since retaining the state of an object or system component in the IoT may actually be useful. Fremantle and Scott went on to note overall middleware security gaps. They noted that no currently available middleware was designed specifically to support privacy and that "none of the middleware systems offered a user centric model of access control," nor were there any that "utilized federated identity at the device level."[19] Therefore, when considering middleware for your IoT solutions, note that privacy is not yet a fully featured or possibly guaranteed part of the middleware feature set. Middleware security should be considered as a gap to be aware of for third-party-vended middleware solutions. As a solution, the authors suggested designers "bring together the best practice into a single middleware that includes: federated identity (for users and devices), policy based access control, user managed access to data, [and] stream processing in the cloud."[20] Best practices are still being developed for middleware security, but the best scenario sketched out above should be attainable in the near future for IoT systems.

Privacy and Security in Location-Based Internet of Things Services

Within the context of IoT location-based services, several key privacy and security measures should be in place before services are broadly available to patrons. Some of these considerations can be adapted from location-based mobile application privacy considerations for the IoT, while other considerations are wholly new for IoT location services. Since the IoT is yet to reach full maturation, several of these solutions will be speculative at this time.

Mobile Technology Security Considerations in Internet of Things Settings

Turning to mobile technology, it is general policy, enforced by the makers of mobile operating systems (Android and Apple), to require that the software ask the user of the app if a location is to be shared. This provides a system-wide enforcement of privacy control, allowing the user to opt out if they do not wish to share their location. There are three fundamental and interconnected actions that take place within mobile technology related to mobile security within the IoT. These include that fact that "mobile nodes in IoT often move from one cluster to another, in which cryptography based protocols are required to provide rapid identification, authentication, and privacy protection."[21] The challenge, though specific to IoT location services, includes the fact that "powered by location based services, IoT systems have the potential to enable a systematic mass surveillance and to violate the personal privacy of users, especially their location privacy."[22] In our Bluetooth low energy (BLE) case study, for example, several novel research questions could be explored, including tracking where students walk in the stacks as they are exploring the path to their item. Sharing the location of an individual in the IoT may not be as straightforward a process as simply asking one app for permission. As shown in the previous chapters, data within the IoT pass through several beacons, servers, and applications—but the notion of consent for location services ought to become commonplace for those services requiring this. For system designers within library settings and researchers in space planning and information science, the paths of users may be of interest for collection layout or even development, but collecting data on users and their paths specifically should be undertaken with consent. The opt-in process ought to be sufficiently clear about what data are collected, how long they are kept, and what they are used for in the purposes of the research study. Within IoT location tools, personally identifiable information should be retained only in rare instances. A better way of gathering data, or managing location data within library IoT location-specific systems, is to generate identifiers that are not directly associated with users, but can still be useful for managing the location service. For location services, it should be possible for users of the service to request any location-specific data that are collected about them. If it is not possible to provide these data, this should be noted in a privacy document regarding the service.

Security of location services and IoT technology is a serious and multifaceted concern. The facets to consider begin with sensors, like Bluetooth beacons. These sensors can be compromised by any vector that first allows system administrators to maintain the system. From our example in chapter 2, a database was constructed of locations of beacons. In rethinking some of the security of the app, this database could be more securely delivered within the app so that there is one less vector to administer and one less vector for possible compromise of security in the system. This adheres to the principle of decentralization, and not only does the patron keep the database of beacon locations secured in their app, any transactions with those beacon data are happening locally. This is a more secure way to serve the app, and at the same time results in benefits to performance in the app—that is, less server read time will result in less latency overall in the location-based service by the user of the app. Another factor to consider beyond the sensor is data that exist or are partially stored temporarily in the cloud.

cloud-based security is relatively well understood, but the cloud represents a possible vector for compromise, and when security is compromised, we know that privacy stands to be compromised as well. Ensuring that personal data are not stored in the cloud could help to mitigate any issues of security if the service is somehow compromised. The cloud could be the place that third-party systems seek to monetize data about your users. Questions should be asked about cloud-based data practices, since in this era of data mining and business intelligence, movements of users as they make assertions about their preferences could be valuable to third-party providers of IoT technology.

Privacy Considerations in Internet of Things Technology for Location Services

The promise for exciting and profound service innovations is one of the driving factors in considering personalized location-based services. When an individual is known to prefer a given location, then better services could be designed based on these personalized data points. Several issues to consider here, though, include the fact that “a user may wish to stay anonymous and may not want to be identified by Location Based Service providers, especially when the information reveals the location of the user.”[23] In the article “A Review of Mobile Location Privacy in the Internet of Things,” Elkhodr and colleagues went on to note that, “While better services can be provided if personalization is allowed, not all Location Based Services require the personal identification of a user.”[24] With regard to institutional attention to privacy considerations, a useful exercise for any IoT service is to have a documented privacy policy for any tools the library is using for location services. Researchers recommend developing these policies for IoT tools as early as possible in the design of the service, since they note that this is a way to gain user confidence and will also help spur the uptake of the service.[25]

Elkhodr and colleagues noted the near impossibility of privacy in the IoT—“The seamless interconnectivity of objects, envisioned in the IoT, highlights the complexity of realizing location privacy in this environment. It is clearly evident that it is almost impossible to achieve perfect privacy as long as seamless communication is taking place.”[26] In essence, there will be data shared by several agents in the system of IoT, and these data will be produced in large quantities without the user knowing where that data finally resides. The authors noted this is particularly problematic with identity information being tied to location information.

Summary of Internet of Things Security and Privacy

To summarize the major factors considered in this chapter, we underscore the need for privacy policies within IoT services. These are especially important when considering location-based personalized service. Since complete user privacy is nearly impossible to assure in personalization services, the requirements for notifying users by way of privacy policies and opt-in notifications are paramount. IoT systems require that library administrators revisit existing patron privacy policies in order to better select services and to protect consumers in this new era of connected technology.

Notes

1. Claire Rowland, Elizabeth Goodman, Martin Charlier, Ann Light, and Alfred Lui, *Designing Connected Products: UX for the Consumer Internet of Things*, 1st ed. (Sebastopol, CA: O'Reilly, 2015), 420.
2. Ibid., 425–26.
3. Ibid., 436.
4. Krista M. Soria, Jan Fransen, and Shane Nackerud, "Library Use and Undergraduate Student Outcomes: New Evidence for Students' Retention and Academic Success," *portal: Libraries and the Academy* 13, no. 2 (April 2013): 147–64.
5. American Library Association, "Privacy," June 19, 2002; amended July 1, 2014, http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy.
6. Bruce D. Weinberg, George R. Milne, Yana G. Andonova, and Fatima M. Hajjat, "Internet of Things: Convenience vs. Privacy and Secrecy," *Business Horizons* 58, no. 6 (November–December 2015): 618.
7. Ibid.
8. Rowland et al., *Designing Connected Products*, 447.
9. Ibid., 449.
10. Ibid., 450.
11. Cricket Liu, "Securing Networks in the Internet of Things Era," *Computer Fraud and Security* 2015, no. 4 (April 2015): 15.
12. Weinberg et al., "Internet of Things," 620.
13. Marshall Breeding, "Issues and Technologies Related to Privacy and Security," chap. 1 in "Privacy and Security for Library Systems," *Library Technology Reports* 52, no. 4 (May/June 2016), 7.
14. Liu, "Securing Networks in the Internet of Things Era," 16.
15. Ibid., 15.
16. Rowland et al., Designing Connected Products, 431.
17. Paul Fremantle and Philip Scott, "A Security Survey of Middleware for the Internet of Things," *PeerJ PrePrints* (July 2015): 9, https://peerj.com/preprints/1241v1.pdf.
18. Ibid., 14.
19. Ibid., 15
20. Ibid.
21. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," *Computer Networks* 76, no. 15 (January 2015): 158, http://dx.doi.org/10.1016/j.comnet.2014.11.008.
22. Ibid, 158.
23. Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung, "A Review of Mobile Location Privacy in the Internet of Things" (presentation, ICT and Knowledge Engineering, 10th International Conference, Bangkok, Thailand, November 21–23, 2012), 268, http://dx.doi.org/10.1109/ICTKE.2012.6408566.
24. Ibid.
25. Sicari et al., "Security, Privacy, and Trust,"152.
26. Elkhodr et al., "A Review of Mobile Location Privacy," 270.