

ALA American Library Association

THE INTERNET OF THINGS

MOBILE TECHNOLOGY AND
LOCATION SERVICES IN LIBRARIES

Jim Hahn

Library Technology Reports

Expert Guides to Library Systems and Services

JAN 2017
Vol. 53 / No. 1
ISSN 0024-2586

Library Technology

R E P O R T S

Expert Guides to Library Systems and Services

The Internet of Things: Mobile Technology and Location Services in Libraries

Jim Hahn



ALA TechSource
alatechsource.org

American Library Association

Library Technology REPORTS

ALA TechSource purchases fund advocacy, awareness, and accreditation programs for library professionals worldwide.

Volume 53, Number 1

The Internet of Things: Mobile Technology and Location Services in Libraries

ISBN: 978-0-8389-5984-8

American Library Association

50 East Huron St.
Chicago, IL 60611-2795 USA
alatechsource.org
800-545-2433, ext. 4299
312-944-6780
312-280-5275 (fax)

Advertising Representative

Samantha Imburgia
simburgia@ala.org
312-280-3244

Editors

Patrick Hogan
phogan@ala.org
312-280-3240

Samantha Imburgia
simburgia@ala.org
312-280-3244

Copy Editor

Judith Lauber

Production

Tim Clifford and Samantha Imburgia

Cover Design

Alejandra Diaz

Library Technology Reports (ISSN 0024-2586) is published eight times a year (January, March, April, June, July, September, October, and December) by American Library Association, 50 E. Huron St., Chicago, IL 60611. It is managed by ALA TechSource, a unit of the publishing department of ALA. Periodical postage paid at Chicago, Illinois, and at additional mailing offices. POSTMASTER: Send address changes to *Library Technology Reports*, 50 E. Huron St., Chicago, IL 60611.

Trademarked names appear in the text of this journal. Rather than identify or insert a trademark symbol at the appearance of each name, the authors and the American Library Association state that the names are used for editorial purposes exclusively, to the ultimate benefit of the owners of the trademarks. There is absolutely no intention of infringement on the rights of the trademark owners.



Copyright © 2017
Jim Hahn
All Rights Reserved.

About the Author

Jim Hahn is an Associate Professor and the Orientation Services and Environments Librarian at the University Library at the University of Illinois at Urbana-Champaign. His duties include developing and evaluating prototype technologies that focus on enabling undergraduates to discover library resources and services that support learning and research and to integrate them into their work. He holds an MS and a CAS in library and information science from the Graduate School of Library and Information Science at University of Illinois.

The author wishes to acknowledge the Research and Publication Committee of the University of Illinois at Urbana-Champaign Library, which provided support for the completion of this research.

Abstract

Drawing examples from a case study of an Internet of Things (IoT)-powered mobile application, librarian Jim Hahn demonstrates IoT uses for location-based services in libraries. The case integrates Bluetooth beacons into an undergraduate library's book stacks. With BLE (Bluetooth low energy) technology, researchers were able to implement a location-based recommender that relies on subject classifications in call numbers that to provide recommendations based on location. Recommendations of digital content like e-books and e-journals can be provided from the context of the book stacks browsing experience. This report explores key technologies for bringing IoT services to libraries, noting especially the privacy and security issues for library leaders, system designers, and users of IoT services.

Subscriptions

alatechsource.org/subscribe

Contents

Chapter 1—The Internet of Things (IoT) and Libraries	5
On Technology and Libraries in the Twenty-First Century	5
Defining the Internet of Things	5
Examples of the Internet of Things	6
Possible Futures of the Internet of Things in Libraries	7
Mobile Technology, Location-Based Service, and the Internet of Things	7
Notes	8
Chapter 2—Indoor Positioning Services and Location-Based Recommendations	9
Wayfinder App Functionality	10
Integrating Beacons into Mobile Apps	12
Modular APIs	13
Recommendations Processing	13
Testing	14
Security	14
Statistical Analysis, Data Storage, and the Internet of Things	15
Case Conclusion	15
Notes	16
Chapter 3—Location Services Technology and the Internet of Things	17
Near Field Communications (NFC) and Location Services	17
Radio-Frequency Identification (RFID) Tags and Location Service	18
Wi-Fi Standards and Location-Based Services	19
IndoorAtlas and Location Service	19
Project Tango Tablet and Location Service	20
Modular Smartphones and Location-Based Service	21
Library Vendors and Location Services	21
Summary of Location Service Technologies	21
Notes	22
Chapter 4—Security and Privacy for Location Services and the Internet of Things	23
General Privacy Considerations within Libraries	24
Security for the Internet of Things	25
Securing Internet of Things Hardware	25
Securing Internet of Things Middleware	26
Privacy and Security in Location-Based Internet of Things Services	26
Summary of Internet of Things Security and Privacy	27
Notes	28

The Internet of Things (IoT) and Libraries

On Technology and Libraries in the Twenty-First Century

Libraries face profound service challenges in the twenty-first century. Some of the challenges relate to changes in the networked information landscape of the last several decades, including the massive and direct availability of information without mediation of a librarian, the challenges associated with curating and describing massive quantities of data, and the renewed challenges related to library as a place combined with perennial questions about the future of print. The intersection and culmination of several of these effects of networks, spaces, and data are poised to disrupt technologies within libraries as the so-called Internet of Things (IoT). The IoT is comprised of billions of connected devices that usher in a new realm of possibility for library service development and innovation.

Some may be wary of the oncoming IoT development since, in no small measure, libraries are asked to do more with less in an age where technology has not always delivered on an upward rising trend of making operations more streamlined or efficient. The implementation of new technologies can, in some cases, even lead to less stable services in the near term as newer services attempt to scale to demands. Technology disruptions do not always end up with the hoped-for result of service efficiencies. There are times, however, when the technological promise is too profound to ignore. Enter the Internet of Things, the latest evolution of networked computing technology, made possible by the ever-smaller form factors of computers and sensors, the combination of which provides a distinctively different, and somewhat unusual, promise. The IoT encompasses very small computers, directly

or indirectly connected and interconnected with the web and everyday objects to provide profoundly innovative levels of monitoring support, device control, service innovation, and, for many, business opportunities.

Defining the Internet of Things

Defining the Internet of Things is a challenge. This challenge is caused in part by the newness of the domain and the many varied services that technologists foresee for the IoT. IoT technologies encompass not just one type of hardware but many kinds of hardware that have existed as unconnected devices. Smart appliances, like networked thermostats or network-accessible “smart ovens” are examples that only begin to scratch the surface of the IoT service possibilities. Several technologists consider the shift to the IoT, where every appliance is networked and has an IP address, as inevitable. The IoT literature goes on to suggest that the IoT will encompass millions of devices linked with the Internet, relating information about environment, logistics, and control systems.¹ Some suggest the IoT will be connected as part of a larger cloud infrastructure that can autonomously collect and produce data about the environment in which it exists. IoT devices are not desktops or mobile devices, but rather computing machines that aren’t traditional end points of use; in other words, the IoT devices do not have traditional interfaces—they are more like probes that gather data.

One reliable source of technology industry reports is Gartner. The company is most likely known to library technologists for its development of the “Gartner Magic Quadrant” research methodology, but

illustrative for our purposes is its helpful and more broadly encompassing definition of the IoT. According to a Gartner industry press release on this topic, “The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.” Noting the economic importance surrounding the IoT, “Gartner said that IoT product and service suppliers will generate incremental revenue exceeding \$300 billion, mostly in services, in 2020. It will result in \$1.9 trillion in global economic value-add through sales into diverse end markets.”² The business applications encompass affordances for efficiency, helping to reach out to new or returning customers.³

For library purposes in general, and the specific IoT library-based case study contained herein, we will use a working definition of IoT that includes how technologies smaller than traditional computing (laptops and phones) will interact with the physical environment. Since early IoT will necessarily have some overlap with what has come before, our case study will talk about how mobile technologies will interface with IoT architectures—namely, beacons that broadcast a Bluetooth signal that help to provide location awareness to modern-day apps.

Yet it should also be noted that, although mobile devices and applications seem an almost natural initial extension and interface into the IoT, there is no requirement that the IoT must be connected to mobile devices in order to provide service enhancement and novel functionality. In the work *Enchanted Objects*, by David Rose, the author noted that small screens, while enabling profound services through mobile device interfaces, may in fact not be the best way to experience connected objects.⁴ Rose noted, “Today we spend most of our technology interaction time staring at little glass slabs, which are positioned right before our eyes and in the center of our focus. This must change. We need to better understand the workings of all five senses so we can involve them more fully.”⁵ The agenda sketched out by Rose is intriguing, since it speaks to ever more immersive and potentially useful IoT uses—that come untethered. In Rose’s perspective, it would make sense to consider the mobile-enhanced IoT environment a transitional state to the more fully encompassing IoT in which devices are less tethered to our control systems of mobile devices, desktops, or servers and act more like the “enchanted objects” described in his IoT vision.

The reason IoT technologies are so hyped today is their promise for a deeper interconnected world and the anticipated benefits that these deeper connections will bring. At least one white paper author has referred to the IoT as “the network of networks” and “the first real evolution of the world wide web,”⁶ and in some industries it looks poised to provide even

deeper automation than is currently possible with unconnected infrastructure.

We pause here to consider the notion that a deeply interconnected world is not new for those in the information professions, which leads us to ask: what is the departure point from library automation and library mobile apps? There is evidence to suggest that the IoT is comprised of small computer resources that are pervasively connected and directly tied to the cloud. If predictions play out as expected, these very small, pervasively networked computers will increase in quantities far beyond desktop, laptop, or mobile adoption. IoT is the culmination of several forces that include ubiquitous computing (like mobile technologies) manifested in the spread of the smartphone, the processing of data streams by cloud-based infrastructures, and the ever-smaller forms of networked computing components.

Examples of the Internet of Things

So far we have covered the idea of smart objects, which can encompass networked appliances. Networked appliances hold the promise of providing additional functionality, convenience, and overall increased standards of living. Take the refrigerator that can order additional supplies of a prespecified food type when supplies go below a predetermined threshold. Beyond the usual examples of smart home appliances like these, the IoT can literally encompass *anything*, leading some to describe the IoT as the Internet of Everything. As an example of the possibilities for an explosion of connectedness, consider the following examples:

- **Environmental monitoring (smart appliances).** There are several examples of consumer products, like the Nest thermostat, that illustrate IoT technology for the home. These devices, by using user input of temperature preferences, can learn over time the habits of the inhabitants of a house and their heating and cooling preferences in order to optimize the preferred temperature for when the occupants are home. Nest thermostats can be paired and optimized further from a user’s mobile device. A mobile app gives the homeowners some ability to control and gather insights about the environment of their home.
- **Smart clothing and smart accessories (wearables)** can send health data to a central server for monitoring heart rate, blood pressure, and similar information. The data could offer predictive analytics into health monitoring. In an article from the Chief Futurist at Cisco, it was noted that within “the next few years, these capabilities will grow profoundly. We’ll be able to swallow a pill

that can monitor our digestive tract and intelligently send relevant information to our doctors at the right time and in the context of what we're doing. Expectant mothers will wear 'smart tattoos' to monitor the health and activity of their babies, and send their doctor an early alert when labor begins. We've only begun to scratch the surface of how wearable technology will transform our lives."⁷

- **Hobbyist projects (Raspberry Pi and other small form factor programmable boards).** There are also many hobbyists interested in the IoT space. When we unpack several of the technologies that come into play in the IoT in chapter 3, we will draw on specific programmable microcontroller board examples. But these small computers have the extensibility to have additional peripherals, such as storage and displays, added to them. There are a range of possibilities for hobbyists in the IoT area. In some ways, these have some of the most interesting applications due in part to the flexibility of the devices.
- **Beacons (Bluetooth low energy).** There are some smaller form factor devices that are enterprise-ready; that is, they have graduated from the hobbyist realm and are available off the shelf in the consumer market. In chapter 2, we'll unpack some of the Bluetooth low energy (BLE) possibilities for location services within the IoT, and in chapter 4, we'll discuss the security implications of beacons that provide location assistance to library systems.

Possible Futures of the Internet of Things in Libraries

The IoT is an emerging area, and several possible services and innovations may become available as a result of an increasingly interconnected networked environment. There is speculation over how its various manifestations will impact our lives and the services we can provide within and outside of libraries. One theorist posited that, as a result of implementing the IoT, "a smart planet will evolve, where many of the everyday things around us have an identity in cyberspace, acquire intelligence, and mash-up information from diverse sources."⁸ The software components needed to make this happen have not yet been developed since most IoT solutions are hardware-based and not federated into intelligence-gathering networks yet. Kopetz also noted that "the novelty of the IoT is not in any new disruptive technology, but in the pervasive deployment of smart objects."⁹ Therefore, it may not simply be a single impact from one IoT technology implementation. Instead, the IoT stands to be a cumulative technology effect due to its pervasive nature.

The hypothetical and supposed IoT benefits to libraries involve issues around how technologists will be able to combine data that might be produced, consumed, or generated from IoT devices to provide innovations in service understanding, which may in fact lead to deeper automation. The data that are produced by inventory control over libraries might in fact help collection developers better understand how users interact with physical spaces.

With regard to the assessment of physical library space, previous to the IoT, there has not existed a good tool kit for knowing what user engagement looked like in collections and in service points at a pervasive level. Beyond assessment, a deeper insight into the actual use of library space will allow libraries to better tell the story of space usage and make decisions based on evidence.

The demand in higher education for evidence-based decision making has never been stronger. While there has been much study by ethnographic researchers who collect qualitative data about what students do in spaces and would like to do in spaces, a deep understanding calls for real quantitative use data about library spaces. There is an actively funded Knight Foundation Project, Measure the Future, which is utilizing IoT technologies for supporting spaces assessment. The Measure the Future project intends to produce hardware and software solutions that will provide a "Google-Analytics-style dashboard for your library building: number of visits, what patrons browsed, what parts of the library were busy during which parts of the day, and more. Measure the Future is going to make that happen by using simple and inexpensive sensors that can collect data about building usage that is now invisible. Making these invisible occurrences explicit will allow librarians to make strategic decisions that create more efficient and effective experiences for their patrons."¹⁰

Mobile Technology, Location-Based Service, and the Internet of Things

Given the technological challenges, how do libraries respond to the IoT strategically and with impact? In this guide, written for the library generalist and those with an interest in technology, we explore a case study of an IoT implementation that makes possible location-based recommendation services in an undergraduate collection, discuss other approaches to providing location-based services, and also give serious consideration to the privacy and security issues associated with such novel technology. The implementation discussed in chapter 2 utilizes commercially available IoT technologies (i.e., proximity beacons deployed in a grid system) in combination with existing mobile device affordance for Bluetooth-based indoor locating.

It is the IoT as it exists today (when this text was written). An implementation of IoT location recommenders may be substantially different one or two years from today, though.

In chapter 2, we explore how mobile technologies can be paired with beacon signals in their environment in order to build an indoor positioning system. Most of us encounter this capability when we connect to Wi-Fi in public spaces like cafés or libraries. We are also familiar with the Global Positioning System used by our phones. Software that delivers real-time directions to our point of interest has generated high service expectations for functionality based on location. With these high expectations, we have found from our iterative tests in the library that students expect real-time location guidance within a building. These studies coincided with new technology startups that have made available technology that made such location-based services possible. In chapter 3, there will be additional attention paid to some of the other approaches that make location services in libraries possible. Several of those technologies include near field communication (NFC) and new Wi-Fi standards. Chapter 4 covers security and privacy considerations for IoT in general and as they relate to personalized location-based services specifically. This open area includes development of securing middleware—that is, the components that comprise and facilitate the interactions among mobile applications and IoT hardware.

As we conclude this introductory chapter, several factors are worth noting. The report, as we have started to suggest, is not only for technology specialists in libraries. The work is intended to be understandable to the library generalist. Therefore, those for whom the IoT is new are encouraged to read on, especially if they have not given the IoT much thought previously. Each chapter can be read individually as well; therefore, while chapter 2 introduces a case study that raises several privacy considerations, if you

are so inclined and motivated, you could go straight to chapter 4 to read about securing and ensuring privacy within the IoT. This work was a wide learning experience for the author, and it is hoped that it can be a learning experience for the reader as well.

Notes

1. Ladan Davarzani and Mark Purdy, “The Internet of Things Is Now a Thing,” *Stanford Social Innovation Review* 13, no. 4 (Fall 2015): 8–10.
2. Gartner, “Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020,” news release, December 12, 2013, <http://www.gartner.com/newsroom/id/2636073>.
3. The Economist Intelligence Unit, *Assessing Enterprise Readiness for the Internet of Things: Executive Summary* (London: Economist Intelligence Unit, 2016), <http://www.eiuperspectives.economist.com/sites/default/files/Assessing-enterprise-readiness-for-the-internet-of-things.pdf>.
4. David Rose, *Enchanted Objects: Design, Human Desire, and the Internet of Things* (New York: Scribner, 2014), 17–21.
5. *Ibid.*, 157.
6. Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, white paper (San José, CA: Cisco Internet Business Solutions Group [IBSG], April 2011), 4–5, http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
7. David Evans, “Beyond Things: The Internet of Everything, Explained in Four Dimensions,” *Impact X* (blog), Huffington Post, September 24, 2013, updated January 23, 2014, http://www.huffingtonpost.com/dave-evans/cisco-beyond-things-the-internet_b_3976104.html.
8. Hermann Kopetz, *Real-Time Systems: Design Principles for Distributed Embedded Applications* (New York: Springer, 2011), 321.
9. *Ibid.*, 307.
10. Measure the Future homepage, accessed July 25, 2016, <http://measurethefuture.net/>.

Indoor Positioning Services and Location-Based Recommendations

This chapter on indoor positioning systems (or IPS) is a case study on a location-based service developed at the University of Illinois Urbana-Champaign. The case involves location-based recommendation through mobile technology paired with commercially available Bluetooth low energy (BLE) beacons. Mobile technologies are a well-suited entry point into Internet of Things (IoT) hardware since mobile phones and tablets by way of their Bluetooth radios offer a way to both communicate with IoT tools and leverage existing mobile services for providing new services. The purpose of this chapter is to provide an example implementation of IoT technologies that responds to a real service need within an academic library setting. Portions of this example will apply to public libraries as well, since larger and more complex book stacks may require additional directional support to items regardless of library type. The example presented here goes beyond simple directional support, however, since it shows a way to recommend relevant digital resources and popular print items from within the print book stacks. As a final preface to this case, note that some portions of this chapter are technical, but no more technical than required in order to explain foundational interactions among Bluetooth beacons, mobile devices, web services, and the custom databases that provide recommendations.

With beacon technology, real-time turn-by-turn directions and real-time recommendations in the book stacks can be provided to a user's mobile device. With the infrastructure and research trajectory developed for an augmented reality experiment, researchers from the undergraduate library at the University of Illinois undertook an experimental project to incorporate Estimote beacons into the undergraduate library book stacks so that students new to the environment

could see the location of their mobile device within the library building through an interactive map on their phone, providing directional support to items and discovery of like items with location-based recommendations.¹ This chapter demonstrates the distributed computing processes and workflows necessary to integrate beacons into collections-based wayfinding and explores the key components for the recommendation algorithm used for “topic spaces” in collections. Distributed systems are common in mobile app development since usually there is a need to serve data from a remote API (Application Program Interface) to a mobile device, like an Android phone. If a remote API is used, this usually comprises at least one remote virtual server communicating with the mobile phone. Sometimes these remote APIs also interact with database data.

These components are listed here as a way of illustrating that components of the distributed system can become multipart. Before moving on to more detail, a comment about the environment within which this API operates: the technology stack used for this case study is heavily Java-based. The Android app is written in Java, the APIs were developed using Java, and specifically the Spring framework was used to generate JSON that the phone would utilize in displaying recommendations.

The experimental location-based recommendation service utilized in this case is grounded in the advantages of collocation that support information discovery and are supplemented with existing ILS data—for example, total circulation of a particular item. The research and development leading up to a popular algorithm was the result of several innovative idea-generating projects that included focus groups with students, user studies of mobile applications in the

library, and interdisciplinary app design competition on the University of Illinois campus.²

Wayfinder App Functionality

This case study uses the Wayfinder module from the Minrva app to illustrate IoT functionality. The Wayfinder module is a part of a larger mobile app platform that utilizes modules to separate different functions of the app for library services. As an example, the Minrva platform includes a catalog search, journal search, account modules for easy renewal, and several branch location custom modules. As an example of a custom module, several library units circulate technology (i.e., loanable technology), such as USB mics and graphic calculators, and since the pool of available devices changes often throughout the day, the technology module was developed so that users of the Minrva app can simply tap the technology module to see a list of currently available technology. From our user studies and follow-on focus groups, the library was able to learn that students are interested in knowing what the popularly circulating technology devices are.³ The request for popularity filters led us to sort the technology items with the most popular items at the top of the list. We use the technology module as an example to illustrate how recommendations are now commonplace as a feature request to add to library services. There are several other custom modules, which can be viewed on the Minrva project catalog list, but the key point to remember is that the custom modules are usually location-specific in order to offer value-added services.

Minrva Project
<http://minrvaproject.org>

Minrva Technology Module
http://minrvaproject.org/modules_tech.php

Minrva Catalog
<http://minrvaproject.org/catalog.php>

Wayfinder is a custom module. Each module is dependent on a unique bibliographic identifier (like the unique key for objects in a database) and is not directly coupled with the larger system of modules. Modules communicate only indirectly.⁴ After a user searches for an item in the catalog search module, they can tap the Wayfinder module to be directed to the location of an item. During user testing of recent Minrva modules, researchers uncovered a user preference of being able to locate their mobile device on the map, not just the location of the selected item.⁵

The focus of our previous study inquired as to how users wished to receive recommendations from stacks-based browsing. Thus, the goals and objectives for using Bluetooth beacons in the book stacks included the following: (a) locating a user's device in the library book stacks, (b) giving a user a recommendation for popularly circulating items, and (c) showing them relevant e-content based on their current location.

The mockup in figure 2.1 demonstrates features of a mobile app that relies on the Estimote beacons to infer its location.

The mockup on the right of the figure demonstrates the recommendations component. There are highly circulating books in this location, but without the assistance of this app the user isn't readily able to discern this, since the information exists only in the integrated library system's reporting database. Researchers designed the business logic in the server so that the service can run queries related to the user location in the book stacks. The popularity query returns print books that are highly circulating in the subject area of this user.

As an additional IoT service, the query by the user's location is returning a variety of e-content that is relevant to the subject area. The e-content that may be suggested includes e-books, online journals, and journal databases that are relevant to the location. It is possible to generate this recommendation by using the subject metadata associated with the book stack range that the user is nearest. These e-resources are not typically brought into a user's navigation of the physical space in the library.

The undergraduate library at the University of Illinois measures 50.8 meters by 56.7 meters and was built underground. The planners for the campus did not want to disturb the oldest operating soil research plot in the country, and they feared a building with a shadow could interfere with the experiment. New undergraduate students must navigate to the lower level of the building in order to locate print items they are interested in. The new and unique building can be intimidating to navigate, and users might suffer from library anxiety. An indoor positioning service that utilizes beacons in order to support navigation of a new, unfamiliar environment is a welcome addition to undergraduate spaces.

The IoT technology that makes locating a user device in the building possible is Bluetooth proximity beacons. The case study at the Illinois site utilized the beacons from a company called Estimote. Fifty-two Estimote proximity beacons were placed above the tiles in the undergrad library.⁶ While IoT technologies are going to vary, the specifics of the Estimote beacons are helpful in illustrating the connectedness of many smaller Bluetooth beacon devices within a native mobile app.

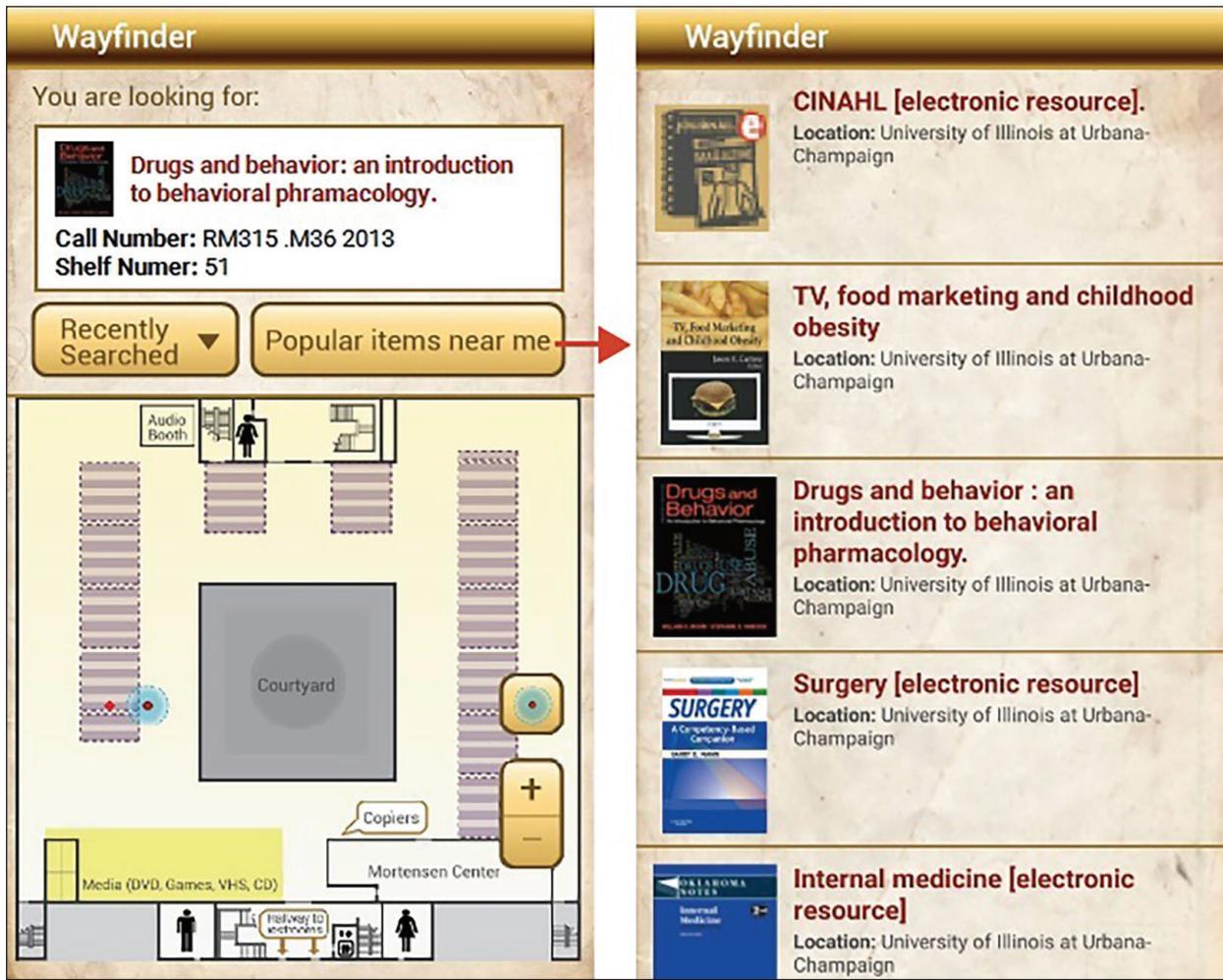


Figure 2.1
The dot with a circle around it is the location of the user's device. The dot within the book stacks indicates the location of the item that the user searched for from the catalog module.

Estimote proximity beacons are comprised of a 2.4 GHz radio using Bluetooth 4.0 Smart, also known as BLE. The Bluetooth beacon does not produce a continuous signal, but rather blinks on and off to alert other devices of its presence. The developer documentation also utilizes an easily understandable analogy for how Estimote Bluetooth beacons function—"You can think about the beacon as a small lighthouse. But instead of light, it uses radio waves, and instead of ships, it alerts smartphones of its presence."⁷ While the Bluetooth beacons from Estimote do feature small, lightweight computers to broadcast a signal, there is not a direct data collection component from the beacons into the Estimote Cloud server. In order to adjust beacon settings—like frequency strength—the user needs to make the changes in the web interface (logging in to the Estimote Cloud) and then sign in to the Estimote app to configure the beacons once the phone with the new configuration is in range of the Bluetooth

beacons. Then the new settings are applied. Both of these steps require authentication as the owner of these beacons. The ownership of beacons is set by Estimote when the order is placed, and it utilizes the customer's e-mail address for ownership at the time the beacons are ordered. We have verified that ownership can be transferred from one e-mail account to another if needed after the beacons have been ordered. This is especially helpful in case one e-mail address is used for a shipping and receiving department and another e-mail address is used by developers for authentication and provisioning purposes. According to the Estimote developer documentation, the Estimote proximity beacons actually have a real-world range of forty to fifty meters.⁸

Once the beacons have been installed in a library building, there is still the step of integrating beacons into mobile apps.

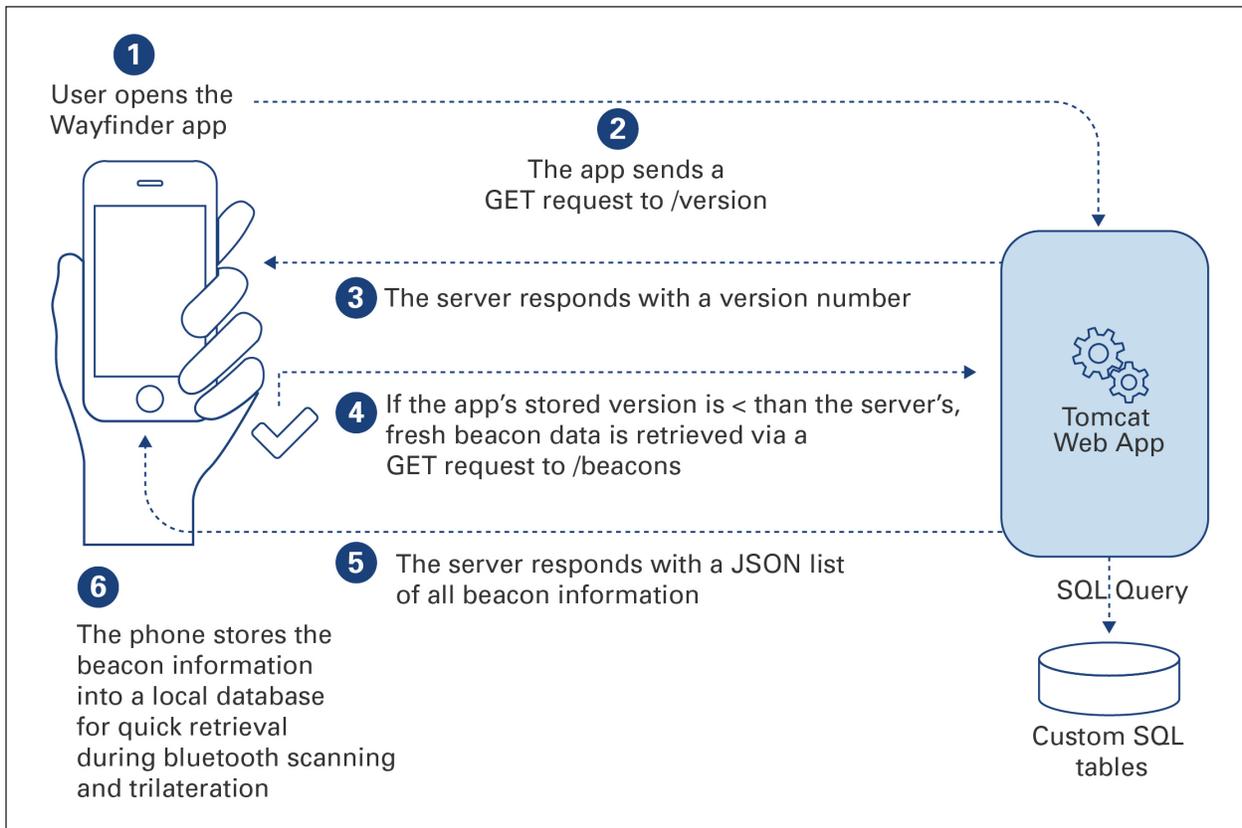


Figure 2.2
An illustration of the data flow from the database of the beacon locations in the grid to the user's smartphone.

Integrating Beacons into Mobile Apps

In our case study, we installed beacons in the ceiling of the library, above ceiling tiles, and adhered to a grid layout of our own design, which divided the library into a 16 by 18 grid. Each beacon was recorded as an x and y coordinate on that grid; device locations were then stored in a small database. The database is a Microsoft SQL: Structured Query Language table that corresponds to the grid system developed over the building's library map. Microsoft SQL is a common relational database tool used in digital library applications. The Wayfinder module loads after a user taps the Wayfinder icon in the larger Minrva app. Upon startup, it checks a web service (in this case, the Minrva Location API) to ensure it has the most recent table of beacon locations (figure 2.2).

Once beacon locations are downloaded to the user's device, there are at least two possible ways for the phone to infer where it is in the building. These are outlined as a way of illustrating design choices and the relative advantages and drawbacks for both. One way developers can make the phone aware of its location is by using the Estimote Indoor SDK. The Indoor SDK has the advantage of including several

novel noise-cancellation algorithms and may be optimized for the device. As an alternative to the SDK, the research team at Illinois has found that a math library for trilateration has provided more reliable indoor location results than the Indoor SDK for Estimote proximity beacons.⁹ This may be due to the underground location or unique environment of many shelves of books, obstacles that likely cause some unexpected interference for the Estimote Indoor SDK. According to the Estimote developer documentation, Estimote engineering believes that the trilateration method may be good enough in cases when the accuracy can fluctuate up to five meters.¹⁰ The reason Estimote developed its own SDK for indoor locating is that it believes that it is possible with several additional methods to get granularity much more precise. Since we have saturated our undergraduate library stack location with the Estimote beacons, we are achieving a better result than five meters.

For the library directional Wayfinder case, the precision needs are not to the exact location of the book on the bookshelf, but are simply to guide a student to a row of books (the shelf of books). The system recommendations will depend on which shelf the user is nearest when they tap the recommendation button on the app. Therefore, precision beyond several

meters is not necessary. Though not utilized in this case, it should be noted that radio-frequency identification (RFID) type systems will provide a unique area of service capabilities by actually guiding users to exact items. This technology will be explored in more depth in chapter 3, which details alternative approaches to location services in libraries.

Modular APIs

As previously mentioned in the introduction to this chapter, the Minrva app is designed as a modular app. Each component part or module of the application uses a specific RESTful (Representational State Transfer) API. RESTful APIs are designed as concise, specifically formatted data produced by programs to be consumed by other programs accessing data over the web. A list of publicly viewable APIs can be viewed on the Services page of the Minrva Project website.

Minrva Services

<http://minrvaproject.org/services.php>

The API that was developed for the Wayfinder module upgrade provides data based on three sources (see figure 2.3): basic call number layout (custom table we curate), searching and filtering (VuFind), and ranking popularity (CARLI reports server).

Examining figure 2.3, we can see first the database labelled as the CARLI Reports Server refers to the Oracle database that is the backend of the integrated library system (ILS). Researchers currently pull all of the data at once through one dynamic query. For production, a service such as this would necessarily require some amount of caching—for example, not directly connecting to a reporting server to get popularity rankings dynamically. In a production system, the technologies may require an immediate response, and this being the case, researchers recommend pulling the data from a prerun report. Reports that store data that would otherwise need to be dynamically

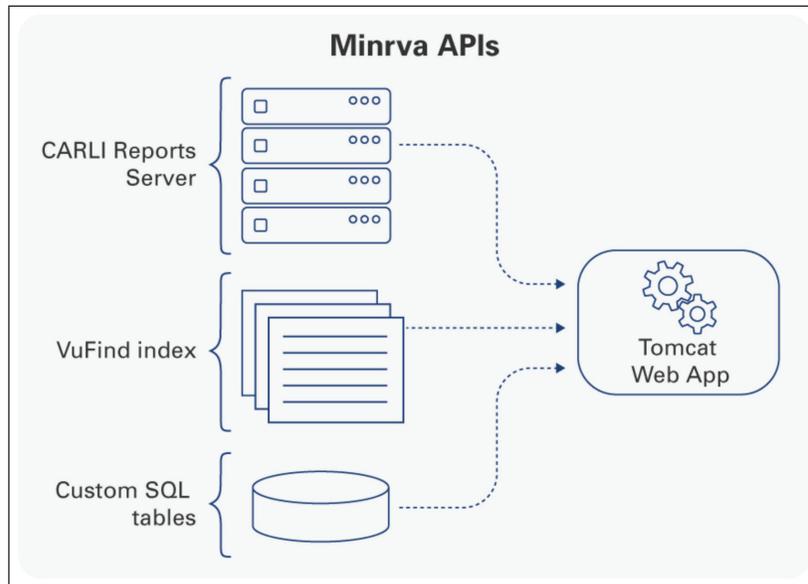


Figure 2.3 Illustration of the databases and data sources that a location-based recommendation service requires.

```
// Get the patron's physical coordinates
PatronLocation location = getLocation(locationInfo);

// Get shelf ranges from Minrva DB, based off of patron location
ArrayList<String> ranges = getRanges(location);

// Get relevant books/ebooks based off of the shelf ranges
BooksDB bookdb = getEBooks(ranges, context);

// Filter and add popular books that are near the patron
List<RecBooksModel> books = bookdb.bookList;

// Filter and add relevant ebooks that would be shelved
// near the user, if the ebook was a physical item
List<RecBooksModel> bookEBook = getPopularBooks(ranges, books);

// Add relevant databases, based off of the patron's location,
// to the list
List<RecBooksModel> bookEBookDB = getDBSuggestions(bookdb.DBList,
bookEBook);
```

Figure 2.4 A demonstration of computing processes that researchers developed in order for the phone to receive the recommendations of print, e-books, and databases.

pulled could run overnight or twice a day as recommendation requirements merit. There may also be value in visualizing these recommendations since their change over time may be of interest to collection developers and system managers alike.

Recommendations Processing

The recommendations processing is the most technical component of the case. In this section, we walk

through the recommendation algorithm. An algorithm, at its most basic and essential parts, is simply a number of functions that represent the steps that the server is taking. These steps are gathering recommendation results defined by a predetermined criterion that will be shown to the user based on the location of their device when they tap the recommendation button (figure 2.4).

In order to process recommendations, the server will filter through functions beginning with the current location. Based off of patron location, we get the shelf ranges from our custom database of all call numbers. Once we know the ranges of a nearby stack, we get relevant books and e-books. We filter for popularity based on that range and add any e-books that would be relevant. Finally, we add any online journal databases that may be relevant to the patron's starting location and serialize this as a JSON response. In order to gather database journal recommendations, the service relies upon an EBSCO article search API. While recommending is not the main purpose of the EBSCO API, the conceptualization of a "recommendation" is considered broadly to encompass those items that are more relevant by arrangement. The API is returning a set of results to a subject query (gathered from the call number). In the case that a single journal title holds most of the results, the service then recommends that journal as being relevant to the subject area. The students still must search within the journal to get articles. This part of the algorithm, at its most basic, promotes the availability of topically relevant journal titles from the EBSCO API. Certainly there are limitations to this type of search since promoting some resources over others may leave out resources that are relevant but not found in the recommendation model.

Testing

Outside of the app, we use Estimote's configuration app to test where beacon sparseness may occur by locating beacons in range.¹¹ With Estimote's configuration app, we can locate areas in the library where beacon reception is sparse and where we might want to add one or more beacons so that there are at least three points to compute—the requirement of trilateration. The more points available to the phone for inferring location, the better the results of computing trilateration.

```

minrva-dev.library.illinois.edu/api/recommend/popularnear?shelfNums=
- {
  bibId: "uiu_6548355",
  title: "Encyclopedia of Buddhism",
  thumbnail: "http://secure.syndetics.com/index.aspx?type=xw12&isbn=9780028659107/SC.GIF&client",
  author: "",
  pubYear: "2004",
  location: "University of Illinois at Urbana-Champaign",
  format: "eBook"
},
- {
  bibId: "uiu_7010231",
  title: "Buddhism and transgression : the appropriation of Buddhism in the contemporary West",
  thumbnail: "http://secure.syndetics.com/index.aspx?type=xw12&isbn=9789047441106/SC.GIF&client",
  author: "Konik, Adrian",
  pubYear: "2009",
  location: "University of Illinois at Urbana-Champaign",
  format: "eBook"
},
- {
  bibId: "hat_819122",
  title: "Christianity and philosophy",
  thumbnail: "http://vufind.carli.illinois.edu/vf-uiu/images/1x1.gif",
  author: "Holmes, Arthur Frank",
  pubYear: "1960",
  location: "HathiTrust eResources (public domain)",
  format: "eBook"
}

```

Figure 2.5

The Android app consumes this JSON to create the location-based recommendations view.

Security

Beacon security for the location-based recommendation system described in this chapter will be primarily handled with the Estimote Cloud. The previously mentioned Estimote Cloud is one way for system designers to ensure that only the owner of the Estimote beacons can change settings. In a real-world environment, if beacon settings are changed by a third party acting to harm the library infrastructure, the beacon battery life could be run down by setting the power level of the beacons too high. As a corollary to this problem, the library's IoT service would also be in danger if a third party somehow managed to set all the power levels of the beacons very low or off. In that case, the system would not function. Therefore, the middleware components that make up some of the valuable connectors of the IoT represent a potential security weak point.

From the example we describe in this chapter, a consumer entity is partially responsible for servers that control how the library administers the beacon settings. This consumer-facing service is not directly secured by the library. These types of IT services are often referred to as "shadow IT"—the tradeoff for management is that the control a department might normally have over infrastructure is lost. This is the tradeoff the library makes in order to utilize an off-the-shelf IoT consumer product like Estimote beacons. Without the infrastructure of the Estimote Cloud, Bluetooth devices that make this possible would have to be developed from scratch. And while there are certainly many hobbyists who experiment with Arduino boards with Bluetooth capabilities or small microcontrollers with Bluetooth broadcast affordances, these would not be a great basis for an enterprise or production service provided by the library. This illustrates

a compromise of several pillars of IT, including standardization and control in order to advance the state of the art in services. If these compromises are to be made by IT leaders in the organization, the author proposes a process of value analysis and understanding how employing strategic technology such as IoT would be meeting strategic service objectives.

After taking precautions to securely protect the Estimote beacons to the extent we are able, there are two additional databases that need to be secured in this case. These are custom databases that the library maintains. The Microsoft SQL database of beacon locations in the library requires security authentication to be put in front of the server. This beacon location database provides the grid coordinates of where the beacons are placed in the library. If the server were breached and the database compromised by a malicious third party that gained unauthorized access to the database, then that party could delete the tables of beacon coordinate data on which the system relies to function. The second SQL table, a call number range database, would also be at risk. Though databases may not technically be an IoT component of the stack, these data are fundamental to the proper functioning of the application. Without securing both the call number database and the beacon location database with authentication, the range lookup could potentially fail, and the system could not properly give the user suggestions based on their location in the building. As we noted in our walkthrough of the algorithm, location-based suggestions are themselves derived from subject metadata that is a component of constructing a call number.

Outside of this specific case, there are general themes to IoT security that are worth mentioning and unpacking with more detail than can be afforded in this case. We hinted at middleware, which is a significant part of the IoT. Connecting many small computers together and deriving service innovation requires a middle component that interfaces with devices like beacons and other tools (like a database) to store or retrieve very large amounts of data to provide value. IoT middleware security will be examined in more detail in chapter 4. As we have shown with the mobile app-based example, the IoT is by necessity a system that interacts with personal computing devices, and so a deeper treatment on security and privacy is necessary.

Statistical Analysis, Data Storage, and the Internet of Things

Assessment is an important component of new service development. Without an assessment plan, it can be difficult to know if a service is actually meeting its intended need. Previous studies of collection-based

wayfinding with mobile technologies utilized formative evaluation methods.¹² These formative methods are well suited for new services such as these, and for IoT technologies, which are new and offer many possibilities, it makes sense to gather feedback early in the design phase, with functional prototypes, so that as the functionality develops it can be vetted with real users in a real-world environment. Formative evaluation in previous mobile app studies was qualitative. However, with Estimote beacons and library server infrastructure, new possibilities for quantitative data analysis emerge.

For this case study, there are some potentially interesting and valuable ways to go beyond traditional assessment, into data analytics and also data visualization. Consider the data analytic possibilities derived from subject-specific and title-specific recommendations that are periodically extracted, stored, and then visualized in a dashboard. Each shelf will have recommendations that will change over time based on what is popularly circulating. Also, e-books are added to the collection over time; as the collection grows and is used, recommendations will also fluctuate. The data analytics component would be suited to collecting and describing this change over time and could provide insights into what types of items users are being recommended as popular, and additionally, if there are gaps in the suggestions over areas that perhaps require more e-content to recommend over time. Finally, if these data are appropriately de-anonymized, the analysis of these data could be made into a shareable dashboard.

Another possible data set that could form the basis for analytics includes storing and visualizing the grid locations where users are seeking recommendations as a heat map. This would help collection managers to understand which areas users are most interested in or which areas of the book stacks are being browsed—and as a visualization experiment, it could also showcase other users' parts of the collection that their peers are finding interesting. These heat maps of where users have browsed in the collection could be visualized on library displays. Display walls in particular would be a possible target of this data analytics and visualization.

Case Conclusion

This chapter has outlined an ongoing research project that details how to integrate IoT technologies into a real-world academic library environment. Utilizing Bluetooth beacons paired with a modularly designed mobile app, library researchers were able to locate the user's mobile device in the building and guide that user to items of interest. As an added benefit, system designers have chosen to implement a location-based

recommender that relies on subject classifications in call numbers to provide recommendations based on location.¹³ These recommendations are novel for library systems since they integrate digital content like e-books, e-journals, and journal databases within the book stacks browsing experience.

Look for future updates from the Minrva's Android or iOS app store presence that will include upgrade details of completed functionality for the indoor positioning service. The development group responsible for this service has posted updates to its project portfolio page, so those who are interested in more details can check back to the Prototyping Group website regularly for additional findings that come out after this work is published.¹⁴

Notes

1. Jim Hahn, Ben Ryckman, and Maria Lux, "Topic Space: Rapid Prototyping a Mobile Augmented Reality Recommendation App," *Code4Lib Journal*, no. 30 (October 15, 2015), <http://journal.code4lib.org/articles/10881>.
2. Jim Hahn and Hillary Bussell, "Curricular Use of the iPad 2 by a First-Year Undergraduate Learning Community," chap. 7 in "Rethinking Reference and Instruction with Tablets," *Library Technology Reports* 48, no. 4 (November 2012): 42–47; David Ward, Jim Hahn, and Lori S. Mestre, "Designing Mobile Technology to Enhance Library Space Use: Findings from an Undergraduate Student Competition," *Journal of Learning Spaces* 4, no. 1 (June 2015), <http://libjournal.uncg.edu/jls/article/view/876/812>.
3. Hahn and Bussell, "Curricular Use of the iPad 2."
4. For more information on Minrva's module system, see Jim Hahn and Nathaniel Ryckman, "Modular Mobile Application Design," *Code4Lib Journal*, no. 18 (October 3, 2012), <http://journal.code4lib.org/articles/7336>.
5. Ibid.
6. At the time of this study, Estimote made available "proximity beacons." However, more recently, after we installed these beacons, Estimote is shipping a new generation of Bluetooth beacons, "location beacons," which promise to be "the most robust" Bluetooth location beacons on the market. There is an all-new software developer kit (SDK) that ships with the new hardware. (Estimote, "Launching the Most Robust Location Beacons on the Market," *Reality Matters: The Estimote Team Blog*, February 24, 2016, <http://blog.estimote.com/post/139902664710/launching-the-most-robust-location-beacons-on-the>.) One would expect the upgraded SDK to provide better indoor location support than the generation launched in 2014.
7. Estimote, "Beacon Tech Overview," Developer Docs website, accessed July 25, 2016, <http://developer.estimote.com/>.
8. Estimote, Developer Docs website, accessed July 29, 2016, <http://developer.estimote.com/>.
9. Trilateration is a process of determining a location given distance measurements of circles. More information can be found on this geometric computation in Wikipedia, s.v. "Trilateration," last modified June 1, 2016, <https://en.wikipedia.org/wiki/Trilateration>.
10. Wojtek Borowicz, "How Do Beacons Work? The Physics of Beacon Tech," *Reality Matters: The Estimote Team Blog*, January 2, 2015, <http://blog.estimote.com/post/106913675010/how-do-beacons-work-the-physics-of-beacon-tech>.
11. "Estimote," Apple iTunes Store, last updated July 22, 2016, <https://itunes.apple.com/us/app/estimote/id686915066?mt=8>.
12. Jim Hahn and Alaina Morales, "Rapid Prototyping a Collections-Based Mobile Wayfinding Application," *Journal of Academic Librarianship* 37, no. 5 (September 2011): 16–22.
13. For a conceptual and technical dive into subject recommendations and location-based services in libraries, see Jim Hahn, "Location-Based Recommendation Services in Library Book Stacks," *Reference Services Review* 39, no. 4 (2011): 654–74.
14. For project next steps on this case study, please see the Technology Prototyping Service project page, University of Illinois at Urbana-Champaign University Library, last updated June 8, 2016, <http://sif.library.illinois.edu>, where technology prototyping project for the library are regularly documented.

Location Services Technology and the Internet of Things

Chapter 1 introduced the Internet of Things (IoT) conceptually. In chapter 2, readers learned of a specific implementation of a Bluetooth low energy (BLE) approach to building location services with recommender features in library book stacks. The BLE beacon approach is only one among several approaches to developing and implementing location services with IoT technology. With the coming maturation of IoT technologies, location-based services in libraries will see increased possibility for service innovation. The maturation and uptake by other industries of IoT-based tools will make additional location-based service innovations possible for library system designers. The future development of consumer-facing IoT tools will have implications for space design in libraries leading toward hyperconnectivity and contextualized services.

IoT innovations will encompass technologies such as near field communication (NFC), radio-frequency identification (RFID), and new Wi-Fi standards. Hardware for IoT systems will move from being a hobbyist concern to a greater mass market and consumer-facing field. Several niche location-based startup companies that leverage sensors within mobile technologies are helping to drive the maturation of IoT technologies. Advances in mobile technology development are also helping to drive IoT systems. These advances include novel modular phones and tablets. In addition to Estimote's example from chapter 2, other startup companies are developing compelling apps and app software development kits (SDKs) in order to leverage new location-based technology.

In this chapter, the ways in which mobile technology can be paired with maturing IoT technology will be detailed, so that examples like those built in chapter 2 can be implemented in library

environments with IoT technologies. This chapter will explore the range of technologies that comprise the tool kit for location services. This chapter provides a foundational introduction to several additional IoT technologies that support location-based services, like indoor positioning systems (IPS) with mobile technology.

Near Field Communications (NFC) and Location Services

One way that most of the readers of this report will be familiar with NFC is from the field of mobile payment technology. Within mobile payments, NFC technology has been used to communicate between a phone and a point-of-sale system, where the consumer's mobile phone connects wirelessly to a point-of-sale system that interfaces with a credit card reader. Apple Pay, as one example, is a technology that relies on NFC in order to process payments from the proximity of a user's pay-enabled device. With regard to location services in libraries, NFC could be utilized to tell a user when they are near another NFC-enabled appliance or device. We will explore later in this section why a user would want to know their proximity to other users in a public space, but it bears underscoring that an NFC device could be another user's mobile phone.

Within special libraries and museums, an NFC appliance could be connected to a special collection's installation. These types of NFC-enabled installations are referred to in the IoT literature as "smart" objects. Smart objects and smart devices are foundational in the IoT literature since "most of the things connected to the IoT are actually simple devices that are often

referred to as *smart devices*. The devices themselves aren't necessarily smart in and of themselves, but become smart when joined together with other connected devices."¹ For the purposes of this text, we are, by design, referencing the ability and capability of Internet-connected mobile devices that connect or communicate with smart devices.

Specific services for special collections in libraries and museums include receiving information when browsing special collections in buildings—for example, NFC-enabled smart objects or smart displays. Special collections are especially suited for NFC interactions. Consider that users of museums are generally visiting multiple content-rich installations about which they may desire additional information. While museums have offered innovative new ways to engage with objects—like iPhone tours and other mobile audio-based information systems—NFC can provide additional information about the object. In newer mobile devices that run the Android operating system, NFC can be used as a data transfer tool. Therefore, a museum could offer a user the functionality to download additional information about a resource, such as archival photos, archival video, or some other interactive content using NFC. This location-based service is content-rich, a feature that might set a display apart from other traditional displays and museum programming.

The Museum of London is doing exactly this type of programming.² The Museum of London NFC implementation allowed users to receive more information about an installation downloaded to their device, offering novel ways to explore and interact. The NFC implementation may also be a faster data transfer and interaction tool when compared to Bluetooth or QR codes for downloading information.

Moving to the more academic services perspective referenced earlier in this section, consider those individuals wishing to form study groups in the library. Traditional group finders in the library did not utilize IoT technology. However, new mobile affordances make finding individuals in a library location easier. This is a desirable service based on previous research into undergraduate students' expectations and needs. The idea for a "Study Buddy" app surfaced during a campus-wide mobile app design competition at the University of Illinois.³ The Study Buddy app design team was made up of student app designers responding to real student needs of finding people in the library who were in the same courses. One of the problems this addressed for students was the desire to know who was in their course and studying in the library—which was sometimes difficult for students to know in large lecture sessions where opportunities to meet others are not possible. Therefore, an NFC-type ad hoc group formation tool is a desirable service for students.

While NFC is a technology that could power an app like Study Buddy, it is not the only piece of technology utilized for this service. An app such as this requires several sets of technologies to come together in order to function. In the case of the Study Buddy app, for example, the app would need to have access to campus locations, be able to manage sessions, and include some type of messaging feature. All of these would need some degree of data persistence, which a database like MySQL could provide. MySQL has been a popular technology component in the past for a variety of library data persistence needs. IoT applications also make use of MySQL software. In the work *MySQL for the Internet of Things*, the author described a process whereby a MySQL server can be installed in a Raspberry Pi node.⁴ The author noted that one of the advantages of this system is that "the low cost Raspberry Pi with an attached USB hard drive makes for a very small-footprint database server that you can put just about anywhere. This is great because IoT solutions, by nature and often by necessity, need to be small and low cost."⁵ The Raspberry Pi is a favorite among hobbyists for the functionality it enables to accomplishing IoT projects. For those unfamiliar with it, a Raspberry Pi is "a small, inexpensive personal computer. Although it lacks the capacity for memory expansion and can't accommodate on-board devices such as CD, DVD, and hard drives, it has everything a simple personal computer requires."⁶ There are several other hardware types that are used in IoT development by hobbyists; these include Arduino boards, among others, but generally fall into the microcontroller set of technology solutions.⁷

Radio-Frequency Identification (RFID) Tags and Location Service

With the incorporation of passive Radio-Frequency Identification (RFID) sensors used as security devices within libraries, the profession may already have a foothold into new IoT location-based services. Most items in libraries that are secured by RFID are secured at the physical item level, something that industries outside of academia and public service functionality are planning to adopt. As Greengard wrote regarding automation and RFID in his work *Internet of Things*: "Inventory and asset tracking technology, often incorporating RFID, identify physical assets or follow them through a supply chain. For more than a decade, retailers have used these systems at the pallet or case level to identify the location of goods in transit. However, retailers and others are now taking RFID to an item level. This makes it possible to build far more robust systems and introduce entirely new features and capabilities."⁸ Greengard noted that there may also be implications in terms of value-added services

that are developed over the technology with “RFID-enabled badges, smartphone apps using GPS and location aware services, and other tools, mak[ing] it possible to know where a person is at any instant. The technology is widely used in secure facilities and labs, including government offices and military bases with strict authorization or access controls.”⁹ Note that Greengard’s portrait of the world is similar to several other predictions related to smarter infrastructure and location tracking. This future vision intimates some of the mass surveillance concerns that are explored more in depth in chapter 4 on security and privacy.

Note, however, that there are examples of ways in which businesses are able to begin optimizing operations through the use of RFID: “A good example of how sensors and monitoring are changing things is apparent in how Swiss-based multinational oilfield service firm Weatherford uses RFID today. The company is able to gauge the condition of drilling equipment and determine when repairs and upgrades need to take place.”¹⁰ At a more library-specific level, consider the environmental areas that need manual reporting when equipment malfunctions—a copier, a scanner, even a personal computer. Consider examples also from larger libraries, which include remote storage areas. Often these high-density remote storage buildings include industrial type technology that could make use of IoT type monitoring tools. Though these types of devices do not yet have RFID-monitoring capabilities, it would be a potential cost-saving measure to see the IoT applied to other types of equipment that libraries own, operate, and maintain—for example, a library with automated shelving units, the type that are designed for high-density shelving. These parts of the library could be equipped with a location-monitoring tool, like RFID, that could record if the equipment was not operating within expected parameters in a given area. This way, shelving systems could be serviced before any breakdowns in equipment occurred.

Wi-Fi Standards and Location-Based Services

Wi-Fi capabilities are getting better over time due to maturing wireless standards. With newer Wi-Fi standards, indoor positioning systems may come integrated into the standard. Indoor positioning services were a novel research area in computer science investigating how to “offer existing Wi-Fi enabled devices a positioning service.”¹¹ With a positioning service in a library building, a library would be better able to support the navigation of complicated or unknown spaces. There is a sustained strand of research in computer science fields on using Wi-Fi as a means to generate indoor positioning services within buildings.

The efforts of applied researchers within libraries has also contributed to advancing the functionality of such services. Several early innovators in this area included libraries in Finland and the University of Illinois Library, which used Wi-Fi access points to determine location within a library location.¹² These services were initially designed to support student wayfinding to books.

There are disadvantages to utilizing older Wi-Fi standards for Wi-Fi-only-based positioning services, since these older standards were not developed for indoor positioning services specifically. However, now that smartphones are more common, the demand for indoor locating is greater, and we may expect future versions of Wi-Fi access points to help support indoor positioning services.

Generally, many of the smart or connected devices that seem to be early IoT technologies communicate with Wi-Fi. Several of the sensors that could collect environmental data—like the Nest Protect smoke alarm system—can leverage Wi-Fi to enable a smart home.¹³ The Nest Protect is a “smart monitor that connects to the accompanying smartphone app via Wi-Fi. At the first indication of any problem, you get a friendly heads-up on your smartphone. If things get worse, the Nest Protect flashes red, sounds an alarm, and tells your household what to do, using recorded words instead of the normal beeps. Nest Protect works in conjunction with the Nest thermostat. If Nest Protect detects high carbon monoxide levels, it notifies the Nest thermostat, which then turns off your gas furnace.”¹⁴ This is an example of how a combination of connected devices can provide location-specific information to a mobile app—but then also act on the information if there is a compelling use case to do so. Similar monitoring of library environments would be compelling in terms on monitoring collections to ensure that proper preservation environments are maintained.

Nest Protect

<https://nest.com/smoke-co-alarm/meet-nest-protect/>

IndoorAtlas and Location Service

IndoorAtlas is a technology startup that developed a solution for mapping local environments in order to provide indoor positioning services using a smartphone. While not specifically designed for libraries, the service addresses wayfinding and orienting functionality for buildings in general. Studies of users new to a building indicate that wayfinding and navigation to items is a problem area for the physical environment, due in part to stacks arrangement and library-based

classification.¹⁵ Specifically, users of spaces may have an information need and have identified a resource, but often struggle from a “last-mile” problem, where they cannot get to the item due to problems with the building and stacks navigation. IndoorAtlas offers a variety of value-added location services for the indoor maps generated by its software.

The IndoorAtlas technology for IPS mapping is original and unique in this area. IndoorAtlas software utilizes the geomagnetism surrounding a building to characterize locations in a room. IndoorAtlas offers a software developer kit (SDK) in order to create several of those value-added services. Utilizing the SDK is a three-step process. The requirements are to first create a venue in the IndoorAtlas web tool, where a floor plan must be provided. Next, the configuration app from IndoorAtlas is used to collect data on the location’s unique magnetic map data. Finally, the SDK can be drawn on to add location-based functionality.¹⁶

Several of the sample use cases described by IndoorAtlas include supporting wayfinding to items in collections. Use cases of IndoorAtlas for installations within special collection or museums include the ability to track users’ experiences in a building in real time. This is also a helpful tool if users need assistance within a collection. A common request in book stacks-based browsing is for real-time point-of-need assistance.¹⁷

Proximity advertising is another area that is drawn from commerce and applicable to museums and library domains. When a user’s device is within the proximity of an object, the SDK can allow for interactions based on these proximity triggers. As a key advantage over several of the technologies in this chapter, the IndoorAtlas technology stack does not require additional hardware—it requires only a mobile phone with app capability. The “multi-dot” feature that IndoorAtlas provides would also help to satisfy the Study Buddy example application detailed earlier in this chapter. With multi-dot, students could opt in to sharing their location with others enrolled in their courses in order to form ad hoc study groups in the library. In larger organizations, the multi-dot functionality would enable employees to quickly locate one another.

To summarize the applicability of IndoorAtlas, note that most smartphones and contemporary mobile devices have standard components like a magnetometer for their compass apps and to enable GPS.¹⁸ IndoorAtlas takes advantage of the ubiquity of the sensors that everyone carries to make possible a unique and simple way to implement location-based service for library needs of locating, navigating, and wayfinding to known items.

Project Tango Tablet and Location Service

The Project Tango Tablet from Google is a piece of hardware that hints at the future of in-building navigation and indoor positioning services. Several novel technologies are combined that make the Tango an innovator within the IPS realm. Within the Tango Tablet, there are increased sensors for depth, which are not included in contemporary tablets or mobile application phones. Within the Tango Tablet are also infrared emitters and an “infrared camera, which picks up the reflected light. A wide-angle camera adds visual cues about location to the mix. The Tango system also relies on highly accurate accelerometers, gyroscopes and barometers.”¹⁹

The library technologist may wonder how exactly these technologies support location services and location-aware apps. According to Elgan, there are several ways in which the Project Tango Tablets actually improve upon beacons for indoor positioning. With the upgraded types of sensors available in a Project Tango Tablet, a mobile device can more readily determine its location within buildings, so apps can better leverage natural markers in the world around the user.²⁰ Lenovo has recently announced that the first “Tango-enabled” smartphone is available for purchase.²¹ With these new devices, there is an increased expectation among users for location services. Google has demonstrated some new advances in indoor location services recently that make use of the Tango capabilities. Tango developers have worked with partners from Lenovo and the museum industry to create indoor navigation with the Tango’s precision sensors for location-based museum guidance and exploration. These features not only include wayfinding and guide tours, but they also implement location-based augmented reality in museums, drawing directional paths onto the real-world environment.²² It is worth noting that researchers in computer science and engineering control systems extoll the advantages of using vision-based approaches to developing indoor positioning services over other techniques.²³ Vision-based services would be much more possible in devices like Tango tablets.

Recent advances in Android software are going to make development for Tango devices easier and more accessible. According to a recent presentation by Tango engineers, Unity engine integration for the devices will make it easier for developers to incorporate augmented reality-type features into mobile services. Features that are being demoed in museums include functionality that provides for step-by-step indoor navigation by overlaying waypoints onto the physical environment through the cameras viewfinder screen.²⁴

Modular Smartphones and Location-Based Service

The modular smartphone concept is related to the Project Tango. A modular phone is a mobile device that has components or modules that can be swapped out and upgraded by the end user.

Note that several of the technologies discussed in this chapter could be pluggable as added components into future modular devices, e.g. an RFID module, a Bluetooth module, a Wi-Fi radio, or even an upgraded camera module to support location services.

Since modular devices may include more than one camera, it may be possible to implement a more compelling vision tool if stereoscopic fields of vision are possible. Current vision-based tools on smartphones actually suffer from only having one forward-facing camera. Depth perception would be possible with a modular phone with two cameras.

Other modular affordances of phones that will support IoT features include sensors, which could be plugged into the phone, so that environmental data that could be collected would expand to include more than what is available on current phones. As an example, current smartphones do not have the ability to read passive RFID, the technology in use within many library settings. However, with a future modular phone, an RFID module could be added to the phone so that as users navigate the collection space, they would be able to learn more about a library collection that included RFID. If items are in their correct location, then the phone would be able show the user where they are located in the stacks. As mentioned earlier in this work, once a location can be inferred, recommendations could be provided to the user, based on their interest. Rather than viewing a map on a screen, the future modular phone could have a way to project its display—either projecting a map or simply projecting an arrow that's overlaid into the physical environment and points to the location of a similar or recommended item. A module of projection capability like the Pico Projector may be feasible for this use case. Such projection capabilities are available in a new modular line of phones, the Moto Z, which includes a small projector as an add-on module.²⁵

On the staff facing side, an RFID enabled modular device could support collection maintenance –e.g. staff walking through the stacks could learn which books are out of order with the wave of a modular phone. This would help optimize traditional shelf reading, but at the same time, in larger library systems, it would be possible to optimize operations by knowing where shelving staff are located. By knowing their location, a colleague or user could route them to pick up requested items in real time. This would help get books to patrons quicker.

And the data routed through the system could help optimize the ways that items are queued for shelving and pick up.

Library Vendors and Location Services

Library vendors are beginning to get involved in the IoT space by way of Bluetooth beacon implementations for mobile enhanced location services. As an example of one vendor, consider the new product Beaconstac offering location services in book stacks.²⁶ According to the June 2016 issue of *American Libraries Magazine*, “Beaconstac uses mobile beacon technology to deliver personalized information to patrons based on their library account and location. To use Beaconstac, a digital beacon location must be set by a staff member at a specific location within the library.”²⁷ This is similar to the system described in chapter 2. Note, however, the Beaconstac would be the company holding data about where a user is in the building. Some libraries may want to host such a solution internally so as to not compromise confidentiality or privacy of library users. Any library using a service such as this should attempt to make it clear what data third parties are collecting, if data are to be collected by third parties.

Summary of Location Service Technologies

To summarize several of the key points and technologies reviewed in this chapter, the technologies that make up the IoT are in some sense already implemented. Therefore, the contemporary IoT is about leveraging new iterations of technologies that are increasingly part of the Internet. Those iterations include feature-rich Wi-Fi, RFID, and NFC. Each of these technologies has its pros and cons when choosing to implement IoT services. As we have seen, hardware is an atomic component of the IoT, but mobile technologies with increased capabilities and functionality make implementing location services easier. This is due to the fact that phones like the Lenovo Tango phone will come with a set of sensors that make hardware-based location services unnecessary. The Lenovo Tango phone is officially known as the Lenovo Phab 2 Pro—the ‘phab’ moniker indicates that it is a hybrid/crossover device, whose size is between that of a phone and a tablet. In summary, there is not a one clear path towards IoT location services. Each of these technologies must be evaluated in the context of a home institution, development priorities, and technology goals.

Notes

1. Michael Miller, *The Internet of Things: How Smart TVs, Smart Cars, Smart Homes, and Smart Cities Are Changing the World* (Indianapolis, IN: QUE, 2015), 9.
2. Museum of London, "NFC at the Museum of London," YouTube video, 1:45, posted August 16, 2011, <https://www.youtube.com/watch?v=QomvjLhYbEo>.
3. Jim Hahn, "The Student/Library Computer Science Collaborative," *portal: Libraries and the Academy* 15, no. 2 (April 2015): 287–98; David Ward, Jim Hahn, and Lori S. Mestre, "Designing Mobile Technology to Enhance Library Space Use: Findings from an Undergraduate Student Competition," *Journal of Learning Spaces* 4 no. 1. (June 2015), <http://libjournal.uncg.edu/jls/article/view/876/812>.
4. Charles Bell, *MySQL for the Internet of Things* (New York: Apress, 2016), 220.
5. *Ibid.*, 249.
6. *Ibid.*, 195.
7. *Ibid.*, 29–78.
8. Samuel Greengard, *The Internet of Things* (Cambridge, MA: MIT Press, 2015), 62.
9. *Ibid.*
10. *Ibid.*
11. Kevin Curran, Eoghan Furey, Tom Lunney, Jose Santos, Derek Woods, and Aiden McCaughey, "An Evaluation of Indoor Location Determination Technologies," *Journal of Location Based Services* 5, no. 2 (June 2011): 2, <http://scisweb.ulster.ac.uk/~kevin/jlbs2011.pdf>.
12. Markus Aittola, Tapio Ryänen, and Timo Ojala, "SmartLibrary: Location-Aware Mobile Library Service," *Human-Computer Interaction with Mobile Devices and Services*, proceedings of the Fifth International Symposium, Mobile HCI 2003, Udine, Italy, September 8–11, 2003, ed. Luca Chittaro (New York: Springer Verlag, 2003), 411–16; Markus Aittola, Pekka Parhi, Maria Vieruaho, and Timo Ojala, "Comparison of Mobile and Fixed Use of SmartLibrary," *Mobile Human-Computer Interaction—MobileHCI 2004*, proceedings of the Sixth International Conference on Human-Computer Interaction with Mobile Devices and Services, Glasgow, Scotland, September 13–16, 2004, ed. Stephen Brewster and Mark Dunlop (New York: Springer Verlag, 2004), 383–87; Jim Hahn and Alaina Morales, "Rapid Prototyping a Collections-Based Mobile Wayfinding Application," *Journal of Academic Librarianship* 37, no. 5 (September 2011): 416–22.
13. Miller, *The Internet of Things*, 101.
14. *Ibid.*
15. Jim Hahn and Lizz Zitron, "How First-Year Students Navigate the Stacks: Implications for Improving Wayfinding," *Reference and User Services Quarterly* 51, no. 1 (Fall 2011): 28–35.
16. IndoorAtlas Dashboard, accessed July 25, 2016, <https://developer.indooratlas.com/dashboard>.
17. IndoorAtlas Use Cases, accessed July 25, 2016, <https://www.indooratlas.com/use-cases/>.
18. J. T. Quigley, "Here's How a Finnish Startup Landed \$10M from Baidu. In a McDonald's," *Tech in Asia*, August 9, 2015, <https://www.techinasia.com/indooratlas-indoor-mapping-baidu-10m-mcdonalds-walmart>.
19. Mike Elgan, "How Google's Project Tango Will Change Your Life," *CIO* (January 4, 2016): 5, Business Source Complete, EBSCOhost AN 112092231.
20. *Ibid.*
21. Lenovo Phab 2 Pro homepage, accessed November 16, 2016, <http://shop.lenovo.com/us/en/tango/>.
22. Lenovo, "Google's Project Tango Reimagines Barcelona Museum," YouTube video, 2:33, posted February 22, 2016, https://youtu.be/P5rRjH_Nhzk.
23. Irene Rubino, Jetmir Xhembulla, Andrea Martina, Andrea Bottino, and Giovanni Malnati, "MusA: Using Indoor Positioning and Navigation to Enhance Cultural Experiences in a Museum," *Sensors* 13 (2013): 17,445–471.
24. Google Developers, "What's New with Project Tango—Google I/O 2016," YouTube video, 39:56, posted May 19, 2016, <https://youtu.be/yvgPrZNp4So?t=32m36s>.
25. See for example the moto "insta-share projector" for the Moto Z line of phones <https://www.motorola.com/us/products/moto-mods/moto-insta-share-projector>.
26. Beaconstac homepage, accessed July 25, 2016, <http://www.beaconstac.com/>.
27. "Streamlined Software: Updated Apollos ILS and Mobile Beaconstac," Solutions: Products and Services, *American Libraries Magazine*, June 2016, 84.

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.

Notes

Notes

Notes

Library Technology

R E P O R T S

Upcoming Issues	
February/ March 53:2	Podcast Literacy: Educational, Accessible, and Diverse Podcasts for Library Users by Nicole Hennig
April 53:3	Information Visualization by Hsuanwei Michelle Chen
May/June 53:4	E-Book Collection Development: A Data-Driven Approach by Melissa Goertzen

Subscribe

alatechsource.org/subscribe

Purchase single copies in the ALA Store

alastore.ala.org



alatechsource.org

ALA TechSource, a unit of the publishing department of the American Library Association