Accelerating Mobile Innovation, Adoption, and Translational Science within a Large Research Enterprise and Healthcare System

Stephen A. Wheat

Institutional mobile application governance and distribution processes are essential to mobile app innovation. The absence of effective processes poses a significant barrier to the development and adoption of mobile apps for use within a research enterprise and also impedes the translational science of applying research apps in clinical and engineering settings. To accelerate mobile app innovation and adoption, Emory University and Emory Healthcare implemented a three-pronged strategy including:

1. Mobile app review and distribution policies and processes
2. Mobile app management infrastructure and mobile app foundation components
3. A strategic sourcing strategy based on preferred mobile app development firms

The results have been an increase from five to 56 mobile apps in the pipeline over three years; increased engagement from technology transfer, legal counsel, compliance, and information security; articulation of a coordinated mobile app strategy; and allocation of more institutional resources toward specific mobile technology and mobile application goals.

Emory Mobile App Policy for Public Apps

Emory's public mobile app distribution policy is owned and administered by the Office of Technology Transfer (OTT) and involves Legal Counsel, Compliance, Information Security, Marketing & Communications, and IT Architecture. The process ensures that a uniform set of information is collected about each mobile app bound for public marketplaces and that a consistent review is performed regarding intellectual property, marketability, liability, terms of use, security, branding, and technical architecture. The policy reads:

"Emory requires an internal review of all mobile applications developed at Emory prior to submission for distribution in public marketplaces, including but not limited to the Apple App Store and Google Play. This process is initiated by the Office of Technology Transfer in consultation with Legal Counsel, Marketing & Communications, and Library and Information Technology Services (LITS). To begin the process, please visit https://wiki.service.emory.edu/x/FqMlAw. As part of the Apple and Google submission processes for public distribution of mobile applications, parties distributing mobile applications must affirm their ownership of the intellectual property and accept marketplace terms and conditions, which include assuming some liability and accepting business obligations. Although Apple spends considerable effort tracking the ever-changing tax landscape, it is possible that errors and miscalculations can happen. If there is an underpayment assessment, the funding for that liability is not covered from a central source of funds. It will be up to the department, unit, or school to fund that expense in the unlikely event it were to arise. For these reasons reviews of the intellectual property ownership status, marketability, and potential liability to Emory are essential."

Emory must also determine if mobile applications collect, transmit, or store any sensitive data and, if so, ensure that Emory's FERPA, HIPAA, PCI, or other appropriate compliance obligations are met. Distribution of mobile applications to any external (non-Emory affiliated) people without completing Emory's mobile application review process is prohibited. Distributing mobile applications that one does not personally own may also be a violation of marketplace agreements." [1]

Mobile App Distribution Process for Public Marketplaces

The Office of Technology Transfer manages Emory's intellectual property rights, oversees industry contracts, and also serves as a single point of contact with industry. Given the nature of the Apple and Google marketplaces for mobile apps, Emory Information Technology identified OTT as the appropriate unit to enter into and manage the distribution agreements with them and sponsor the mobile app submission, review, and distribution process [2].

Step 1: Request Internal Distribution of the Application. Mobile apps must first be distributed to the internal Emory reviewers using the Emory Mobile App Catalog, a type of internal Emory app store. App owners complete the Internal Mobile App Distribution Request Form to start this process. These requests are generally completed within two or three days.

Step 2: Office of Technology Transfer Intellectual Property Analysis. OTT requests that an intellectual property disclosure be completed for all inventions at Emory [3]. The disclosure process collects basic information about the invention: purpose, description, intellectual property ownership, funding, and resources used in development, etc. While OTT uses this information to perform an assessment of the marketability of the invention and how best to protect the intellectual property, other stakeholders use this information to assess legal, branding, compliance, information security, and technical aspects of mobile apps.

Step 3: Marketing and Communications Branding Review. The Emory Office of Marketing and Communications established that all mobile apps that are Emory's intellectual property will bear the Emory name and marks and be branded as Emory apps unless there is a compelling business reason for alternative branding. Marketing and Communications maintains guidelines for branding of mobile apps and advises app owners on how to incorporate the Emory logo, name, and other marks into the app.

Step 4: Legal Counsel Review. The Office of Technology Transfer consults with Emory Legal Counsel on the outcome of the intellectual property review in Step 1 and reviews specific plans for distributing or commercializing the mobile app. OTT and Legal Counsel develop appropriate terms of use.

Step 5: Compliance and Regulatory Review. Compliance with the Health Insurance Portability and Accountability Act (HIPAA) is a major concern for health sciences and healthcare organizations in the United States. HIPAA Title II requires implementation of secure access to electronic health information by specific types of organizations. Emory University and Emory Healthcare compliance officers review mobile apps to determine if Emory's compliance

policies, including HIPAA, apply. In general, these guidelines are used to determine if HIPAA applies to a mobile app.

1. HIPAA applies when the mobile app provides Emory clinicians access to personal health information (PHI) for billable patient care.
2. HIPAA does not apply when the mobile app collects, stores or transmits PHI only for a user's personal use.
3. HIPAA does not apply when the mobile app provides researchers access to PHI for research or non-billable care. However, Emory security policies/practices may still apply (See #5).
4. Any application that collects, stores, or transmits PHI must implement appropriate information security measures even if HIPAA compliance does not apply.
5. When designing, developing and distributing mobile apps, a list of mobile app defaults and security related questions must be considered, as defined by Emory Information Security policy [4].

Step 6: Technical and Information Security Reviews. Emory Information Technology and Information Security review the information provided in the app submission to determine if an in-depth technical security review is warranted. If uncertain or substantial risk is evident in the submission, Information Security performs an in-depth security risk assessment and makes risk remediation recommendations to the owners of the app. The app owners ultimately have the responsibility to remediate or accept the risks identified.

Step 7: App Marketplace Submission. Emory IT works with the app owner to collect the copious metadata and collateral such as descriptions, images, screen shots, etc., required to complete app marketplace submissions. Emory IT digitally re-signs apps for public distribution and submits the apps using Emory's official marketplace accounts. Emory IT then relays feedback from submission reviews to the app owners and developers until the app is accepted for distribution in the public marketplaces.

Emory has a project manager who maintains a mobile app dashboard, which lists all apps and their status in the process at the following stages [5]:

1. Concept, Cost Estimation, Design, or Development
2. Under Review for Public Distribution
3. Under Review for Internal Distribution
4. Publicly Distributed Apps
5. Unreviewed, Unapproved, Publicly Distributed Apps
6. Internally Distributed Apps
7. Retired Apps
8. Retired Unreviewed or Unapproved Apps

This status dashboard with a detail page for each application helps project management and app owners move their apps through the review and approval process [6]:

Emory Mobile App Policy for Internal Apps

Emory's internal distribution policy is owned by Libraries and Information Technology and involves Legal Counsel, Compliance, Chief Medical Officer and Quality Officer, Information Security, and IT Architecture. This policy and its processes are focused on translating innovative apps from research applications into appropriate clinical and reference apps in a manner consistent with Emory's quality goals and priorities. The policy reads:

"Emory requires a review of all internal mobile applications at Emory (developed at Emory or vended) prior to distribution to end users for production use. Internal mobile applications are those intended for use by Emory people and Emory affiliates only and not segments of the general public. This process is initiated by LITS in consultation with Legal Counsel and the Emory Healthcare and Emory University Compliance Officers. To begin this process, please visit https://wiki.service.emory.edu/x/7ILaB. While internally distributed mobile applications do not have the same business and branding requirements as publicly distributed mobile apps, internal mobile applications have many of the same legal, compliance, and security implications. For this reason, Emory must perform a technical review, compliance and regulatory review, and a security review for internal mobile apps. Mobile applications may be distributed internally to a limited user base for development and testing purposes prior to this review, but the reviews must be completed satisfactorily prior to distributing apps for production use.

Emory requires that all internal mobile applications developed at Emory, both native apps and mobile web apps, be distributed for production use using the Emory Mobile App Catalog. Mobile web apps may also be distributed by communicating a uniform resource locator (URL) or a launch web page in addition to listing them in the Emory Mobile App Catalog. This practice helps ensure that Emory can track mobile app usage, apply security policies, manage application updates, and otherwise support the applications. Some vended mobile apps may require distribution by the vendor or distribution through a public marketplace. These practices for vended applications are allowed when they do not introduce unmanageable risk to Emory.

Emory requires a review of all apps available in public marketplaces that are listed for download in the Emory Mobile App Catalog. The process for reviewing mobile apps endorsed by Emory and listed in the Emory Mobile App Catalog is initiated by the LITS in consultation with Emory Healthcare and Emory University Compliance Officers. To begin this process, please visit https://wiki.service.emory.edu/x/suIGBQ (the same process as the Vended Apps in the next section). These mobile apps are endorsed in some way by Emory when they appear in the Emory Mobile App Catalog and they should be reviewed and documented to indicate the nature of their review and recommended or *endorsed* use." [7]

Mobile App Distribution Process for Internal Apps

LITS is responsible for internal distribution of Emory mobile apps. LITS implemented an abbreviated process for internal distribution of Emory apps. A streamlined process was possible because Emory has fewer app branding requirements and more focused legal and compliance requirements for internal apps than public apps [8]. The steps of this process are:

Step 1: Request Internal Distribution of the Application. Mobile apps must first be distributed to the internal Emory reviewers using the Emory Mobile App Catalog, a type of internal Emory app store. App owners complete the Internal Mobile App Distribution Request Form to start this process. These requests are generally completed within two or three days.

Step 2: Internal Posting Review. LITS is responsible for the high-level technical review process to determine necessary security and compliance reviews (e.g. any applications collecting or storing PHI, payment information or compliance-related data). If these reviews are required, owners are notified of relevant policies, practices and considerations.

Step 3: Compliance and Regulatory Review. Compliance officers from either Emory University or Emory Healthcare determine which compliance policies apply.

Step 4: Technical and Information Security Review. Technical review teams from either Emory University or Emory Healthcare conduct a technical review. If additional steps or materials are required, the organizer notifies the developers to prepare for the necessary deliverables and next steps. If a security review is required,

the Emory Information Security team will meet with the developers to walk through a structured security checklist for all relevant requirements – security, compliance and regulatory. If uncertain or substantial risk is evident in the submission, Information Security performs an in-depth security risk assessment and makes risk remediation recommendations to the owners of the app. The Emory business unit responsible for the app ultimately has the responsibility to remediate or accept the risks identified.

Mobile App Infrastructure and Architecture

With these policies articulated, Emory was able to identify and fund infrastructure and resources to support these processes including: a mobile app catalog or internal app store to distribute apps internally and review apps ultimately bound for public marketplaces, staff to administer the app catalog, and staff to administer the review process.

Emory researched and evaluated mobile app management platforms and mobile device management infrastructure in a 2014-15 assessment and concluded that a mobile app management approach was best suited for Emory at that time. Mobile app management focuses on managing app distribution, management, and security policies at the application level on devices that are not under institutional control. Mobile device management places devices under institutional control to implement distribution, management, and security policies. Emory determined that over 99% of the mobile devices on its network were not institutionally owned devices, but rather devices that were owned or managed by individuals, commonly known as bring your own device (BYOD). This realization focused Emory on mobile app management as the most appropriate and significant solution to mobile app distribution at Emory. During this assessment Emory also learned that its mobile user base was approximately 82% iOS and 18% Android, or disproportionately biased toward Apple when compared with the general public or global market analysis, which are essentially inverted with Android at over 80% market share [9].

Emory identified a much smaller, but essential need for mobile device management infrastructure to manage sets of devices that are owned or issued to specific individuals, but used in kiosk or check-out settings in venues like clinics, museums, and instructional settings. Roughly three hundred devices were identified in this category. These devices need to be provisioned and refreshed on regular intervals and updated automatically with new releases of apps to support their functions in educating patients, guiding tours, or providing research materials.

Emory selected Apperian EASE to implement the Emory Mobile App Catalog for mobile app management and distribution to Emory BYOD devices (or 99% of devices) and implemented this infrastructure as an enterprise-wide service. The remaining 1%, which are kiosk or check-out devices, are managed by AirWatch within the units who own each pool of devices in a decentralized manner. Emory has considered implementing AirWatch mobile device management as a central service, but the relatively small number of kiosk and check-out devices presently used in this manner makes an enterprise-wide service of this type a low priority.

Emory implemented the Emory Mobile App Catalog in 2014 as a proof-of-concept and operationalized it as a production enterprise service in 2015. Emory purchased a software-as-a-service solution called Apperian EASE, which was acquired by Arxan in 2017. The solution provides the following core functions for Emory:

1. Presents both mobile apps that Emory develops and mobile apps Emory uses to Emory people in one place
2. Automates the complex signing and distribution process for mobile apps
3. Allows authorized app owners and administrators to distribute mobile apps to Emory users quickly and efficiently
4. Supports distribution and feedback on applications during development and beta testing cycles
5. Restricts access to specific collaboration groups or distributes to all Emory people
6. "Hybridizes" mobile web apps to operate and appear more like native apps
7. Provides a comprehensive set of security and deployment lifecycle policies Emory administrators can apply to apps to implement important aspects of the app lifecycle such as automatically updating apps and critical security and compliance aspects such as requiring authentication, copy-paste-protection, jailbreak protection, etc.
8. Enables curation of mobile apps into categories that are of particular interest to cohorts of Emory users

One of the most surprising discoveries Emory made in implementing mobile app distribution is the extent to which users expect to get mobile apps from an app store or app catalog. This experience appears to be a defining attribute of the mobile experience for many users. Emory has developed and purchased a number of mobile web apps or web applications that have mobile-optimized views. Business owners of these apps request or in some cases adamantly insist that these mobile web apps, which are accessible from any mobile browser with a link, be hybridized with Apperian's hybridizer and be distributed through the Emory Mobile App catalog so end users have a mobile app experience and get a mobile app icon on their home screen. One business owner of such an app even stated that their department promised their users a mobile app this year, and if they just send users a link to an app they can view on their phone, it is not a mobile app. The extent to which users associate an app store or app catalog experience with being a mobile app was surprising, but makes sense when one considers that most users build this expectation from their many interactions with either the Apple App Store or Google Play.

The Emory Mobile App Catalog is a successful service currently with 1,760 users across Emory University and Emory Healthcare and delivering 62 mobile app deployments. Emory tracks mobile app catalog users and mobile app deployments in the app catalog as two of the key metrics of the process and success of its strategies. Figure 1 illustrates the growth in Emory App Catalog users over the past three years [10].

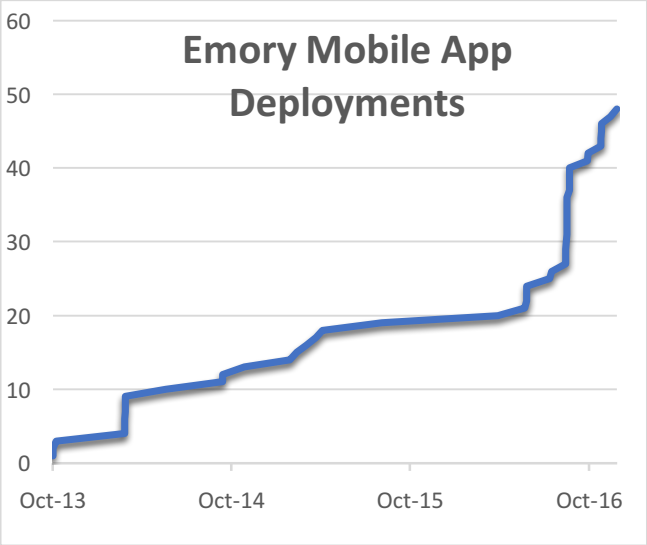

Figure 1: Emory Mobile App Deployments from 2013 through 2016

The number of app deployments performed in the app catalog grew commensurately over the same period [11].

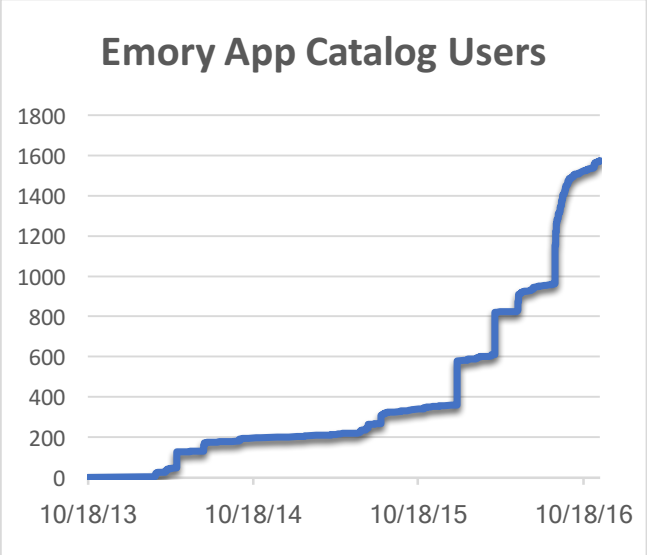

Figure 2: Growth of Emory App Catalog Users from 2013 through 2016

In addition to the Emory Mobile App Catalog as infrastructure Emory invested in two significant areas of mobile app architecture: mobile app authentication and service-oriented architecture. These are critical enablers for mobile apps because they are hard for small research projects or mobile app consultants to implement on their own in a manner that is compatible with Emory's security, compliance, and architecture requirements.

Emory implemented and documented an approach to using SAML 2.0 authentication, specifically with Emory's Shibboleth SAML 2.0 identity and service provider infrastructure. This pattern and attendant infrastructure can be used for any internal mobile app project with an internal Emory user base.

In order for Emory mobile apps to access institutional data, they must consume WSDL-described SOAP services which implement all of Emory's security and auditing requirements. This can be challenging for many developers more accustomed to RESTful services without complex authentication mechanisms or message structures. In order to help developers consume these services more readily, Emory extended the OpenEAI message object API generation infrastructure, which generates a clean Java object API for these services, to generate an Objective C API for use in iOS applications as well.

Both of these authentication and service-oriented architectures work well at present, but they are only a small part of the total architecture Emory will require. The breadth of infrastructure required and the burden of maintaining it for rapidly evolving mobile operating systems compelled Emory to look at frameworks that were more sustainable. Amazon Web Service's Mobile Hub implements backend features and generates client-side Swift, Objective C, and Android projects replete with all necessary APIs to call that infrastructure. Emory is presently working through a detailed evaluation of AWS Mobile Hub and anticipates that this infrastructure will be far more comprehensive and sustainable than the frameworks used to date.

Strategic Sourcing of Mobile App Development

Emory's remaining challenge to mobile app innovation has been inadequate staffing for mobile app analysis and development given the unpredictable timing of research funding. To address this deficit, the institution is working with several mobile app development firms that are capable of working within preferred mobile app architecture and security frameworks. The goal is that these vendors will become proficient in assisting Emory units with accurate cost estimates for proposal budgets and the implementation of funded projects.

Mobile apps are costlier to develop, test, and maintain than one might think. There are many reasons for this:

1. Most mobile apps require both a front-end user interface (what you see and interact with) as well as back-end services for logic, storage, and integration with other applications. Few mobile apps turn out to be stand-alone apps. Even basic content apps often require an integration with a content management system to maintain the content efficiently and effectively.
2. Mobile app platforms are complex and evolving rapidly, requiring frequent testing and often rework of apps to function on new releases of mobile operating systems and devices.
3. The mobile app development tools and developer ecosystems are constantly evolving and changing. This means that mobile app developers and deployers must keep current with these changes.
4. Many times, administrative mobile or web features are required for administrative users or other roles that may not be foreseen in the functional design goals for end users.
5. Security is paramount for apps with a back-end exposed to the internet. At Emory if the data is subject to compliance policies this may prescribe very specific security measures and audit requirements that must be implemented.

It is not uncommon for a simple mobile app for iOS and Android to cost US $50,000 to develop and US $20,000 per year to maintain and operate. A complex application can easily range in the hundreds of thousands to implement and maintain annually. Given these costs it is imperative to get meaningful estimates for projects from the beginning. Useful estimates help in preparing budgets for grant proposals or allocating institutional funds for the project.

One of the primary challenges for mobile apps at Emory has been funding. This challenge has three dimensions:

1. Funding to perform meaningful estimates to start
2. Funding development and implementation
3. Funding on-going operations and maintenance of the app

The challenge of funding meaningful estimates is that less than 15% of the projects LITS has helped estimate have been approved for funding, either by research grants or institutional resources. In performing initial analysis and effort estimation to adequately prepare proposal budgets, the institution effectively does this work for every project when only one in seven is funded and implemented.

To address this challenge LITS has developed a method to reduce the effort of the estimation process while still producing enough artifacts to make a meaningful estimate that can be validated by other developers. For apps from low to medium complexity, this process usually involves three or four 90-minute meetings with a project team and approximately 20 hours of effort between meetings for a total of about 25 hours of effort. LITS is working with preferred mobile app development firms to duplicate this type of assessment process at a reasonable cost.

The market rate for 25 hours of effort for these assessment resources is roughly US $4,000. LITS has been offering these assessments free of charge to Emory units, but has limited capacity to provide them ongoing. LITS produces written use cases, data structures, and in some cases user interface wireframes are required for novel aspects of the app.

The technical goal of the estimation process is to identify significant factors that impact the cost of all mobile apps and to gather enough information about the function and features of the app to estimate its unique costs. Specifically, the process attempts to determine:

1. The user base(s) of the app (internal, external, roles, etc.)
2. How the app will be distributed (internal app catalog, public marketplace, etc.)
3. Platforms of the app to reach its user base(s) (iOS, Android, Web, etc.)
4. What other apps are available for a similar purpose, function, and user base(s)
5. Primary use cases for each type of role in the user base(s)
6. Key data structures the app queries for, creates, updates, and deletes as well as the nature of that data (sensitive, non-sensitive, health information, etc.)
7. Critical application and validation logic that must reside on the backend (so all clients can access it uniformly)
8. Details of complex, unique, or unusual user interfaces suggested by the use cases. Many common UIs can be easily estimated from stories, but others may sound easy yet be quite complex—this step specifically attempts to draw out those complex pieces for more details and estimation.

Once complete, the research group or business unit can use the estimate to seek grant funding or budget institutional funds to implement the project. Once funded, Emory identifies institutional app developers and project management resources or selects a vendor from a list of preferred mobile app vendors. Emory presently has very few qualified internal mobile app developers and these resources are challenging to hire and retain, so strategic sourcing from preferred contracting firms is imperative. This aspect of the mobile app strategy remains untested as Emory has just started outsourcing projects to strategic partners. However, two projects with two well-established vendors have been successful. Time will tell if this strategy is reliable and scalable in the long term.

In conclusion, Emory's three-pronged strategy of mobile app policy, infrastructure, and implementation resources increased its ability to support researchers and clinicians in their endeavors to develop and apply mobile technology. The strategy helped align institutional resources to promote mobile development safely and securely. The dramatic increase in Emory's mobile app distributions, mobile app users, and mobile app portfolio support that conclusion. and helped align institutional resources to promote mobile development safely and securely.

S. A. Wheat is with the Libraries and Information Technology Department of Emory University, Atlanta, GA 30322 USA. He is also with IT Architecture for Emory Healthcare, Atlanta, GA 30322 USA and the Atlanta Clinical & Translational Science Institute (e-mail: swheat@emory.edu).

***Keywords*—**Mobile App Management, Mobile Device Management, Mobile App Governance, Mobile App Distribution.

[1] Emory University, Policy for Emory Public Mobile App Distribution, https://wiki.service.emory.edu/x/8ILaB (Adopted October 14, 2014)

[2] Stephen Wheat, Emory Mobile App Review and Distribution Process for Public App Marketplaces, https://wiki.service.emory.edu/x/FqMlAw (Last Updated June 7, 2017)

[3] Emory University, Technology Transfer Disclosure Forms, http://ott.emory.edu/forms (Posted June 5, 2014)

[4] Emory University, Mobile App Security Defaults, https://wiki.service.emory.edu/x/uQlFBQ (Last Updated December 17, 2014)

[5] Emory University, Mobile Application Review and Approval Dashboard, https://wiki.service.emory.edu/x/7oYcBg (Last Updated May 11, 2017)

[6] An example mobile app detail page showing the status of an app in the review process is Emory University, Public App Approval Details – SUGARx, https://wiki.service.emory.edu/x/v4UcBg (Last Updated May 9, 2017)

[7] Emory University, Policy for Emory Internal Mobile App Distribution, https://wiki.service.emory.edu/x/8ILaB (Adopted November 17, 2014)

[8] Stephen Wheat, Emory Mobile App Review and Submission Process for Internal Emory Distribution, https://wiki.service.emory.edu/x/7ILaB (Last Update: February 10, 2017)

[9] Chance Miller, Latest Gartner data shows iOS vs Android battle shaping up much like Mac vs Windows, https://9to5mac.com/2016/08/18/android-ios-smartphone-market-share (August 18, 2016)

[10] Emory Internal Data, Emory Mobile App Deployments from 2013 through 2016

[11] Emory Internal Data, Growth of Emory Mobile App Catalog Users from 2013 through 2016