ECAR working groups are where EDUCAUSE members come together to create solutions to today’s problems and provide insight into higher education IT’s tomorrow. Individuals at EDUCAUSE member institutions are invited to collaborate on projects that address core technology challenges and advance emerging technologies important to colleges and universities. More information can be found at the ECAR working groups website.

Introduction

The extraordinary success of apps for mobile devices has brought a new dimension to the higher education environment. As of July 2015, between Apple’s App Store (for iOS) and Google Play (for Android), over three million apps are available to download. To put that in perspective, over 1,100 apps per day would have to have been added to these marketplaces since the introduction of the App Store in July 2008. Never before have higher education’s IT communicators and stakeholders had to confront such a combination of new hardware and software, with external entities controlling the delivery, upgrade, and maintenance of those technologies.

To provide services to and engage with constituents, higher education has evolved into institution-sanctioned app development. But with that move, questions around governance arise, particularly as the apps are made available in public, third-party app stores. For example, what qualifies as an institutional app? What brand and design requirements are specific to apps? Are there processes to ensure an app is tested for quality assurance, as well as security and legal requirements protecting student privacy? How is intellectual property determined when apps are developed by students or faculty? Are there financial considerations? Educational institutions must address these and other challenges and opportunities as the use of mobile devices and apps across campus continues its exponential growth.

Governance exists not only to protect the institution but also to provide a service for mobile app creators and users alike. Although governance has been defined as “The decision framework and process by which enterprises make investment decisions and drive business value,” mobile app governance serves a greater purpose of ensuring quality, usefulness, and functionality; maintenance of user security and privacy; efficient publishing to app stores; and, when necessary, appropriate action to update or unpublish apps.

Further complexity exists in institutions that are highly distributed or that may be struggling to manage the explosion of consumerized new technologies. Some opt to take over maintenance of student-built mobile apps, while others grapple with the complexities of in-app payments made to the institution and the distribution of collected funds. Yet others have developed robust testing procedures for all apps before they are submitted to the native app stores.
Mobile app governance defines best practices and provides clear guidelines for app development and publishing. This paper focuses on mobile apps directly related to the educational institution and downloaded through an app marketplace for the purpose of providing a service to the institution.

**Governance Structure**

A typical mobile app governance structure consists of a team of people and a set of policies or procedures guiding simple, efficient, and effective production of institutional apps—those developed internally as well as relevant third-party apps. The development of a governance structure depends on a few key elements: governance goals, the app products themselves, and the app development process.

**Mobile App Governance Goals**

The structure of app governance should be guided by defined goals. For example, a primary goal may be to “produce mobile apps aligning with institutional strategic priorities,” potentially with secondary goals, such as “apps we produce will be secure” or “apps we produce will add value to the university/college experience.” Because these goals may overlap with those of existing institutional governing bodies, mobile app governance could be integrated into or extend the scope of an existing governance structure. For example, existing governance for institutional websites could also incorporate mobile app governance if their goals are similarly aligned. If an incorporated governance is not feasible, modeling mobile app governance on existing governance, informal processes, or departmental-level approaches takes advantage of existing structures.

**Pre-Governance Apps**

Many institutions support apps that were created before governance existed. When developing mobile app governance, you may need to develop special considerations for these applications, including questions of grandfathered apps, how to work with apps that don’t comply to the new guidelines, etc.

**Mobile App Products**

Apps can vary widely in function and purpose. Differing functions mean different app requirements for a governance structure to accommodate. Most apps allow users to consume information such as news, events, and other institutional information. Other apps may be used to securely add or generate content, such as completing expense reports. Other apps may focus on a particular segment of the institutional population, such as research tools. All of these uses have the potential to involve both sensitive and restricted data (see below for more on data security and privacy).

**Mobile App Development Process**

Mobile apps are software and usually follow the typical life-cycle stages of application development: identify a need, develop/create, test, and publish. These phases should also inform a governance structure. Ideally governance would be structured to have a role within each of these phases of development, covering the lifespan of an app from inception to decommissioning.

If a newly formed mobile app governance body is created, it should help the institution adapt to rapid changes in mobile technologies and user expectations by providing a focal point for the mobile governance, development, and deployment process.
A governance charge defines the structure’s purpose and responsibilities. It will outline the kinds of applications that fall under the jurisdiction of the governance. For example, will governance address both campus community and convenience apps—such as bus routes, campus map, or dining facilities—as well as instructional apps for courses? What about oversight on research apps?

**Governance Scope and Team**

The mobile app governance team is responsible for:

- Facilitating executive buy-in to mobile app governance policies and processes
- Leading a consolidated and streamlined process for review and approval of institutional mobile apps to be made available in public app stores
- Ensuring that appropriate stakeholders are represented in decision making
- Establishing processes and policies around:
  - Determining what qualifies as an institutional app
  - Branding requirements
  - Advertising
  - Legal considerations
  - Development and maintenance
  - Privacy, security, and compliance
  - Distribution via app stores

To best represent the spectrum of interests at play, the governance team should comprise a wide range of stakeholders, each with distinct areas of expertise. Each member of the governance team represents an area of expertise. For instance, technical representatives ensure the app is developed securely, while communications representatives ensure that it meets institutional requirements related to design, user interface, and marketing and promotional language. Beyond the core team, additional stakeholders may be called on as necessary to assess the app within their bands of knowledge. While technical concerns are especially critical, an app’s content, presentation, and—most importantly—purpose as it relates to benefitting the user should also take priority. A well-balanced team will reflect a broad base of concerns—from user expectations to assessing app usefulness and institutional priorities—as well as a range of issues, from branding/marketing to legal issues and technical requirements. Depending on a particular app’s function, knowledge from additional stakeholders may also be required. Table 1 identifies key stakeholders likely to be involved in a governance team.
Table 1. Mobile app governance stakeholders

<table>
<thead>
<tr>
<th>Unit/Stakeholder</th>
<th>Role/Responsibility</th>
</tr>
</thead>
</table>
| Information Technology (IT)              | ▪ Manage technical review and security audits of apps  
▪ Assess code/compiling and keys/certificates  
▪ Manage testing and ongoing maintenance  
▪ Maintain app store presence               |
| Marketing/Communications                  | ▪ Ensure that apps follow guidelines for naming, branding, and design  
▪ Check for editorial/language consistency |
| Institutional Review Board (IRB)          | ▪ Ensure adherence to responsible research practices                                                                                                   |
| Hospital, Medical Center/College of Medicine | ▪ Work to ensure that HIPAA and human-subject concerns are met                                                                                      |
| Legal                                    | ▪ Review and sign off on EULAs, app store contracts, and vendor RFPs                                                                                |
| Technology Commercialization             | ▪ Assess commercial viability/pricing and potential for technology licensing  
▪ Monitor licensing, intellectual property usage                                               |
| Academic/Faculty/Student Services        | ▪ Determine strategic direction  
▪ Provide concept validation and development resources                                            |
| Students                                  | ▪ Provide user testing and feedback  
▪ Create student-developed apps*                                                                                                                          |

* Student-created apps may come from individuals or arise out of student clubs. See, for example, "Rutgers Student Club Develops Apps for the University Community," "App-titude: Students Innovate with Mobile Apps," and the University of Maryland Mobile App Developers Club.

To build institutional knowledge, an ideal team has dedicated or standing members and meets (or communicates) regularly or as necessary to move apps through the process. Since team members likely will have other responsibilities outside app governance, rotating the chair of the group may help distribute workload across the team.

**Governance Processes**

Governance processes facilitate that the app creator’s goals align with those of the institution. In the case of mobile app governance, a creator’s goal is to have institutional apps “published” within the institution’s main public app stores. The institution’s goal is to publish apps aligned with its strategic principles. Governance processes create a set of steps or workflows to accomplish these goals. In the absence of a defined governance process, app approval may occur informally, without oversight or guidance, potentially after the app has been developed. For example, approval may be initiated by an e-mail from someone who wants to get a new app into the stores. Without institutional coordination, a managing unit
may not know whom to contact if the app falls out of sync with OS upgrades or if other issues arise. It is therefore essential that governance processes be communicated broadly (often in concert with clarifications regarding the purpose of the mobile governance committee), particularly at institutions where distributed development is common and in the cases where apps may be published under institutional subbrands (e.g., athletics) so that the processes are clear in the development stages rather than when the apps are ready to be submitted to the public stores. Figure 1 models a mobile governance process by which mobile app creators can take part in an informational session with privacy, security, and IT governance representatives before submitting the app for full review.

Figure 1. Recommended process model for governance

The mobile app governance team will need to decide how to prioritize its review workload. Some apps are tied to specifically timed events on campus—such as orientation, graduation, or a planned research deployment—and therefore may need to jump to the top of the queue based on deadlines. In addition, mobile governance processes may vary depending on which institutional group developed the app. For instance, many institutions have published apps that were built by faculty, staff, students, or external developers. Externally developed apps almost always have an internal sponsor that will typically shepherd the submission process along.

Now let’s take a look at the details of establishing processes and policies in the scope of governance.
Determining What Qualifies as an Institutional App

An app governance team may be tasked with assessing whether an app belongs within the institutional family. Given the often complex relationships between higher education institutions and with corporate/private partnerships and sponsorships, there might never be all-encompassing rules to make decisions. Case-by-case assessments may be necessary, but some general questions might be useful to ask when making a determination: Is the app creator faculty, student, or staff? Is the owner/publisher acting on behalf of an institutional department or unit? Does the app’s purpose and function align with an institutional priority, strategic goal, or academic pursuit? Do the app’s intended users align with the institution’s constituency (e.g., students, faculty, alumni, patients, etc.)? For a given app, if the answer is “yes” to a majority of these questions, there is likely a strong case for publishing it under the institution’s app store account.

Branding Requirements

Consistency is a key component of brand identities. It’s common for institutional websites and print materials to make use of common colors, fonts, and design elements to achieve a familiar look and feel. All general-purpose apps representing the institution should adhere to the same guidelines used by other communications vehicles. App governance should ensure that general-purpose apps follow the institutional branding guidelines. However, branding requirements may not apply to all apps, such as those developed by subbrands of the institution (e.g., athletics) or research apps that are the combined effort of multiple institutions.

Apps may even require their own specific set of brand elements or guidelines. Ideally, the institution will use a specific development platform that takes into account and provides recommendations for standard app elements. Resolutions and formats can vary by platform and change over time to account for new devices—for example, the pixel density of Apple’s Retina display requires high-resolution logos and graphics. Graphics templates for common elements can help speed up an app’s design process.

In addition, app stores—such as iOS App Store and Google Play—have their own of required formats and dimensions for marketing imagery and text appearing within an app’s listing on the store. The prescribed formats tend to evolve with changes to the stores, OS updates, or new hardware releases. To help app developers who may not be current with changing store requirements, the governance team should maintain up-to-date guidelines and, when necessary, recommend updates to app templates and resources provided within a brand set of digital assets.

Advertising

Mobile app governance may require that apps posted to the institution’s public app stores align with institutional policy. It may be the case, for instance, that your institution has a policy disallowing advertisements on the institutional website. This may then be applied to mobile, ensuring apps within the institution’s brand are held to a uniform policy standard. At other times, an institution may decide that allowing advertising in an app is akin to allowing ads in the student newspaper.
Legal Considerations

In addition to making the mobile apps useful to the consumers, developers must consider legal issues. It is important to know that mobile apps fall under both online laws and telecommunications laws because apps are delivered on a mobile device and use the Internet.

What end-user license agreement is used for institutional apps?

Most developers defer to an app store’s default end-user license agreement (EULA), particularly if the purpose of the app is simply to distribute information. However, depending on the app type, an app might need a specific EULA. The choice of license agreement for any institutional app will be driven by the needs of the institution to adequately protect itself and its intellectual property. There is not a single standard to use for licensing mobile apps. Both Apple and Google provide standard license agreements for apps made available through their respective app stores, but app publishers can substitute their own agreements, provided that they meet certain requirements. If a standard agreement is used, care should be taken to ensure that the agreement satisfies all institutional legal requirements.

It is worth noting that, unlike desktop software that will often prominently display the EULA when the user first launches an application, the same cannot be said for mobile apps. The trend of most mobile developers has been to minimize focus on the EULA and focus on the user experience. Although an app’s license is published on the app’s page in each app store and can be added somewhere in the app’s interface, it is rarely presented when first launching the app. This may not present a concern for most institutions. However, if end-user awareness of the EULA is important to the institution, effort needs to be made to alert users when they use the app; it is not realistic to believe that end users will seek out and read the license before using the app.

How are intellectual property and payment to creators handled?

App ownership should comply with the institution’s intellectual property policy regarding software authorship. In many cases a disclosure of the software creation is made to the office of intellectual property, and rights are then negotiated on a case-by-case basis.

Apps with different financial profiles may need to go through different publishing/approval processes. For example, a free, public-facing app can be simpler to publish in app stores than a commercial, public-facing one. Commercial institutional apps (those that have a purchase price attached to them) likely need to be reviewed by the institutional intellectual property/technology transfer office. Both the Apple and Google app stores charge an overhead on all app sales of 30%. So, for example, if the cost of an app is 99 cents, the app store takes 29 cents and the account holder gets 70 cents. Because of the fees levied by the app stores, some institutions allow app creators to receive app-generated revenue up to a certain cap (e.g., $150,000) before any of the revenue is shared with the institution.

Development and Maintenance

As with any software, the development and maintenance of apps require careful forethought and follow-through. Moreover, as with any web-development initiative, mobile app development involves key steps such as requirements gathering, analysis, design, development, testing, deployment, and the critical feedback loop from usage. In addition to the usual development challenges, mobile apps must also
consider the unique features of the devices and platforms they support, differences in how each mobile platform’s navigation and standard user interaction functions differ, and so forth.

What are your testing procedures and quality-assurance processes?

It is important for the institution to have a reliable set of apps in the store that accurately deliver the functionality that they say they will. Some of the design considerations made for the implementation drive the mobile application test-planning and test-case scenarios. It is critical that all users (personas) have a positive experience every time they use the app and that the functionality is effective in its purpose.

Some key considerations in building test-case scenarios include:

- Devices and OSs supported
- Unique device features
- Security requirements
- Functionality
- Speed
- Data consumption
- Impact on battery life

Once the test criteria are determined, the app must be tested across all of those metrics. Testing options include:

- **Testing with devices**: In addition to testing using the emulators built-in with the development platform, additional testing should be performed using actual devices. These efforts can prove to be labor intensive and expensive. For internally developed apps, the university should set a policy on who is responsible for completing quality assurance procedures. However, if an external entity has developed the app, the testing may be even more extensive.

- **Staffing**: Quality-assurance testing related to security, privacy, and functionality is estimated to take between three and six hours per app (the time varies due to the significant scope and functionality spectrum from app to app).

- **Feedback**: If the app is discovered to have significant issues, it should be sent back to the creator to remedy the issues and later resubmit it for review.

- **Community development**: Sometimes apps are developed by creators outside the IT organization. These may include students, non-IT staff, faculty, and others. In these cases, additional consideration needs to be given as to whether the institution has the ability to maintain the app over the long term. The key question in this scenario is whether the donated app has an institutional sponsor or stakeholder who is willing to take ownership of it.

Does the governance process require app code to be shared and/or versioned in a specific way?

Because apps are software, they should be treated as any other software solution. Therefore, you should look to your organization’s standards on code sharing, versioning, and ownership. These can range from
individual or departmental solutions to centrally supported, fully documented solutions. If student or nonprofessional creators participate in app development, they should be held to the same governance process to ensure consistency and adherence to best practices. It is highly advised that app code be developed and that a code repository such as Git be used.\(^5\)

**How does the institution manage mobile apps developed by vendors or third parties?**

Mobile application development requires specialized resources and skills. Rather than take on this complexity itself, an institutional unit may wish to outsource the creation of an app to a reputable and experienced third-party developer. It’s recommended these apps follow the same governance processes used for internally developed apps. But mobile governance can and should facilitate a third-party app development project in a number of additional ways:

- **Selection:** Governance should maintain a list of qualified and approved external vendors, especially those who already have a successful working relationship with the institution. A preapproval list gives units a head start in finding an external development partner suited to the app’s requirements, budget expectations, and project timeline.

- **Estimation of sanity checking:** A mobile governance team can lend its expertise to the unit, helping assess whether the vendor’s interpretations of the project scope, deadlines, and cost estimates are realistic and align with the work to be performed.

- **Third-party publishing considerations:** Early in the project, determine the preferred method to publicly distribute the app. Some vendors may prefer—and have a business model to support—the distribution of an app via their own store or a store created on behalf of the unit. If no governance rules prevent it, this may be a convenient route for the unit but requires a greater level of institutional trust with the vendor. It will be necessary for governance to work with the vendor to clearly define institutional access to the store for maintenance/updates and analytics.

- **Code-signing considerations:** Governance rules may mandate that an app only be published through an institution’s public or private store. To prove authenticity, apps published to an institution’s store must be compiled from source and signed with the institution’s unique store certificates. Depending on an institution’s governance and security rules, it may not be possible to share institutional certificates with a vendor. Vendors typically provide the compiled version of the app for the university to submit to the app store. To avoid a potential impasse, as early as possible determine vendor willingness to provide the app’s uncompiled project source code. Some vendors may be reluctant to do this if they are building apps upon their own proprietary system using their own intellectual property.

**Once an app is published, how are app updates and code maintenance managed?**

Holding mobile app development to the same standards as all software development is critical. Like all software, mobile apps have significant dependencies on the operating systems they are built on. Without a maintenance plan, apps built specifically for a particular device (native apps) will quickly become unusable. As app complexity increases, the likelihood that an OS update will break the app also increases.
Understanding app reach and impact with analytics

Analyzing even basic usage metrics may help determine if developing an app was worth the time and effort. Spending the time upfront to understand the goals and outcomes of your app will help answer these questions. Once you have established the goals of your app, analytics can measure success. Some app stores provide analytics, while others may require additional development effort. Analytics in app stores typically tracks the number, frequency, and geographical location of downloads. Additional metrics worth tracking include the number of times a certain view is shown to the user or the number of times a user taps a specific button. Analytics data that directly map to a goal or outcome should be tracked through your own methods.

Is a process for sunsetting or decommissioning apps needed?

Apps should be withdrawn from the stores if they fall out of maintenance and the sponsor can no longer maintain them or if they are superseded by newer apps. In addition, apps intended specifically for research purposes should be considered for withdrawal when the relevant study has been completed. Ideally the governance team will proactively monitor the life cycle of apps within the stores it manages rather than relying on app creators to report when an app has outlived its usefulness.

Privacy, Security, and Compliance

The mobile app governance process needs to manage privacy principles and security risks, with a primary focus on the data collected or exposed by the mobile app and the state and federal regulations that must be satisfied. In addition, all mobile apps will need to be reviewed to ensure compliance with ADA requirements.6

What data can apps collect and process?

Governance guidelines may advise practices for collecting and using protected data, such as grades or class schedules.7 Depending on the type of data, specific legal restrictions, such as under FERPA or HIPAA, might also apply. In addition, apps that work with research data or are developed for research purposes will need to comply with existing IRB requirements.

Some apps may use SMS as a means to collect data. It is important to note that SMS traffic is not considered deidentifiable because it can be traced back to a phone number and thus to a person. IRBs typically advise use of nonidentifiable logins so people cannot be traced.

Finally, if the app will be used in a foreign country, the app creator may need to consult with campus export-control experts. Certain countries might impose data-use restrictions, and U.S. developers may be prohibited from using certain types of encryption when creating and publishing apps.

Medical Schools and Centers

Working on mobile health apps has become an energetic activity at many research medical institutions. Some large organizations may need to have a separate coordinating body just to track these efforts. The desire to leverage electronic health record data requires a secure application program interface (API) and more sophisticated app architecture.
What security requirements need to be met?

The security review of a mobile app is essential, particularly as one considers the increased risk posed by mobile device theft and compromised apps. The type of data distributed or collected in an app determines the security requirements and protocols used. For example, mobile apps that incorporate HIPAA data need to be fully encrypted, in local storage, in transit, and at rest. Many apps use the same encryption that most websites use when they leverage security key certificates as in a website using HTTPS. It’s important to note that apps incorporating texting functionality (SMS) are not secure.

Is there a privacy policy requirement for institutional apps?

As with websites, apps published to stores should adhere to an institution’s existing overarching privacy policies. Additionally, app owners should be strongly encouraged to make the app’s data usage—what data are being collected and how they will or will not be used—known to users.

Are apps allowed to authenticate and/or authorize users?

Depending on what authentication/authorization services are available on a campus, mobile apps can leverage these services in much the same way that websites use web services. Regarding authorization/authentication, many apps for research that collect data have authorization schemas built into the server side of the applications. These communications are encrypted through the use of the SSL protocol. Further, many of these apps use generic IDs that are connected to the user only through physical, handwritten (i.e., not digital) consents.

Distribution via App Stores

Because apps are distributed through an app store developer account that serves to represent the institution in that store, it is important to understand the choices available to an institution and what each choice will ultimately result.

Which app stores to support?

Institutions typically decide what app stores to support based on their student population. Google Analytics, surveys, and governance committees are most often used to determine which devices students are using. A large percentage of institutions are at least publishing to both Apple’s iOS App Store and Google Play. Paying attention to analytics over time is important because the market may change as new devices are released; responsibility for this may fall to the governance committee or the department that manages the app. Most institutions are not staffed to support all platforms, so choosing the options based on your population is the best bet. Depending on the app’s audience, it may be beneficial to bypass the public app stores and instead distribute the app internally using institutional resources, such as a login-protected website. Products exist to allow an institution to create its own “enterprise” app store, with the ability to restrict app availability based on policies, affiliation, and device platform.

Use Case: CASA on Rails

UCLA has recently begun to leverage an open-source community app sharing architecture called CASA on Rails. Distributed app creators from the campus community can log in to submit their app for review, view their submitted app’s status, publish to the native app stores, and include their app in the “UCLA Mobile” app catalog environment.
How do you manage your app store presence with reviews and imposter apps?

Customer reviews from the app store are not being managed for most institutions. This is a decision usually based on available resources. A few institutions have an office or team of students who monitor the reviews and rankings. A number of tools are available that can track rankings, reviews, and downloads or other sales performance metrics if you don’t want to track these measures manually. Students increasingly report issues to the app store and sometimes to your helpdesk. It is a good practice to have someone monitoring app feedback on a regular schedule.

Most mobile app governance processes do not monitor app stores for infringing or imposter apps and accounts. At some institutions, employees or student employees monitor app stores for infringing or imposter apps. At institutions that do monitor app stores, remediation for infringing/imposter/inappropriate apps and accounts is typically handled with cease and desist letters or the involvement of legal counsel. Anecdotal evidence suggests that after a few cases of infringing/imposter/inappropriate apps and accounts are addressed, recurrence drops significantly.

Who owns and may publish to the official account?

Because setting up and maintaining an app store account requires time and effort, institutions may be hesitant to allow each department or development group to have its own account. Further, some app store vendors want to minimize the complexity of multiple accounts per institution. Additionally, both the Apple and Google stores allow only one account to use the official institution name. Therefore, it has been the best practice for each institution to have only one official, institution-sponsored account. However, this can become problematic when multiple groups want to publish with that account. Depending on the culture of your institution, the mobile governance committee can consider whether it is better for all app creators to have access to the account and be able to publish at their convenience or for one central group to manage the account, with others working through that group to get apps published. The best solution will ultimately be what works best for the constituents at your institution.

The first model—of allowing everyone who does app development to have access to the account—is best suited for highly decentralized organizations. This allows each separate organization to publish, update, and manage its apps without needing to go through a centralized process. However, there will still need to be one organization responsible for communications with the app stores for support and renewal.

A centralized model works well for larger or highly centralized institutions. Although this requires more policies and governance, it can help maintain a higher standard of apps by providing oversight and a more formalized publishing structure.

Conclusion

Mobility is becoming a mainstream expectation, and higher education institutions need to have broad strategies for accommodating the desired consumption patterns of the communities they serve. Governing the usage of institutional mobile app store accounts will allow institutions to have more cohesive presences in these environments, as well as help keep the institution in compliance with ever-evolving privacy, security, and branding policies.
Authors

Special thanks go to the following ECAR-APP Working Group authors of this report:

**Jim Burgoon**  
Director, Interactive Communications  
The Ohio State University

**Deepika Chalemela**  
Director, Digital Technology  
University of Texas at Arlington

**Jason Fish**  
Director, Teaching and Learning Technologies  
Purdue University

**Brett Pollak (Co-Chair)**  
Director, Campus Web Office  
University of California, San Diego

**Rose A. Rocchio (Co-Chair)**  
Director, Mobile and Web Strategy, Education and Research  
UCLA

**Jeffrey Rosczyk**  
Lead Web & Mobile Apps Developer  
University of California, Santa Cruz

**Shady Shehata**  
Principal Data Scientist  
D2L

**Lori Tirpak**  
Executive Director of Enterprise Systems  
Oakland University

**Matt Willmore**  
mobileND Program Manager  
University of Notre Dame

**Robin Ying**  
Vice President for Information Systems  
Tidewater Community College

Additional thanks go to the following:

**Theresa Semmens (Contributor)**  
Chief Information Security Officer and Director, Records Management  
North Dakota State University

**Christopher Matthew Ward (Reviewer)**  
Director of Web Services and Mobile Development  
Kennesaw State University

For more information about this paper and ECAR working groups, contact Karen A. Wetzel, Program Manager, EDUCAUSE.

**Citation for This Work**

ECAR working group paper. Louisville, CO: ECAR, December 18, 2015.
Notes

1. “Android users were able to choose between 1.6 million apps. Apple’s App Store remained the second-largest app store with 1.5 million available apps.” See Number of apps available in leading app stores as of July 2015.


3. Many institutions—particularly those that teach mobile-apps development courses—have “internal stores” for apps. The governance being discussed in this paper applies only to apps that are being put into public stores. At times, apps that have already been built and put into internal stores may then become candidates for public stores and will need to then go through the governance process to address issues of quality, long-term maintenance, and intellectual property, among others.

4. See Apple’s Instructions for Minimum Terms of Developer’s End-User License Agreement and Android’s App Licensing.

5. See Git.


7. For information on data classification—identifying protected classes of data—see the 2014 Information Security Guide Data Classification Toolkit.