Web and Mobile Device Application Evaluation and Recommendations

Prepared by Brookline Surveillance and Military Type Equipment Committee

Introduction

More and more today people, organizations and governments and their departments rely on the use of information technology to provide goods, deliver services and to go about our daily lives. A big part of this is the use of applications (apps) that exist on mobile and other computing devices. This is true for the Town of Brookline. The issue of how to evaluate applications and the need for a policy that can be used town wide was a charge given to the Surveillance and Military Type Equipment Committee. This brief report provides some initial guidance on how to acquire and use apps and the policy and procedures around their use.

Recommendations

In all cases the use of apps should go through a process that is represented in the following diagram. Importantly, and as the first step, the decision to use and app should be vetted by the proper individuals who have responsibility for the evaluation and acquisition of these applications. As a general framework this should include the town's Chief Information Officer (CIO) office and the administrator of the individual department information technology (IT) system, the department that procures this IT capability as well as legal counsel. (see the following diagram). This process should be consistent across the town as bespoke policies for different department can introduce risk. This does not preclude the need for compliance with specific requirements of a given department as part of the review. For example, requirements about payments or reporting about use of information about children would need to be including in examining the compliance requirements for an app in addition to the overall policy for evaluation of the apps themselves. The process also needs to be easy to follow to avoid, "going around the system" because it is too cumbersome and does not allow access to tools/apps that can address real needs.

It is recommended that consideration of the long-term stewardship, storage, maintenance, and deletion of the data (including metadata) generated by applications take place before downloading and use. The dissolution of a company or a change of ownership can create a situation where control of information and the agreement and terms and conditions of the data sharing can change. Again, this needs to be considered up front in to avoid unwanted consequences later.

Special consideration should be given to any redirection of information that takes as part of an application. It should be made clear prior to any information flows taking place and where the data will ultimately reside and who is the beneficial owner.

As part of the committee's work we have added a specific set of privacy considerations to the vendor vetting questionnaire that is used to revaluate application, cloud services and information technology vendors.

We recommend that residents follow guidance on best practice. There are numerous references to follow, the National Cybersecurity Alliance, among others provides resources to online basics. There are more technical references at the end of this brief document.

OK for use
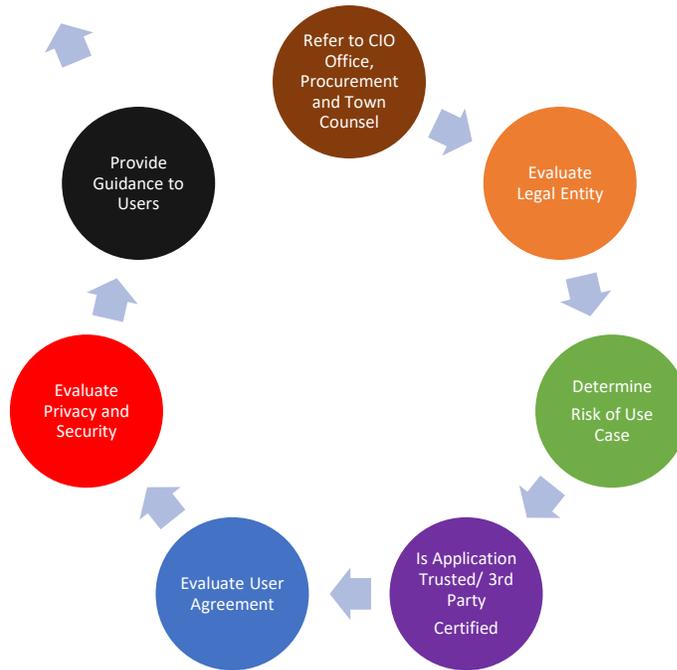
There are multiple frameworks that exists for the evaluation of apps. The **following is an example for evaluating** *health applications* **from reference 1.**, which then contains another 11 references for application evaluation. This framework goes into some of the details for evaluation are the "OK for use" stage at the end of the cycle above and is specific in its references to health information (medical claim) but can be generally applicable.
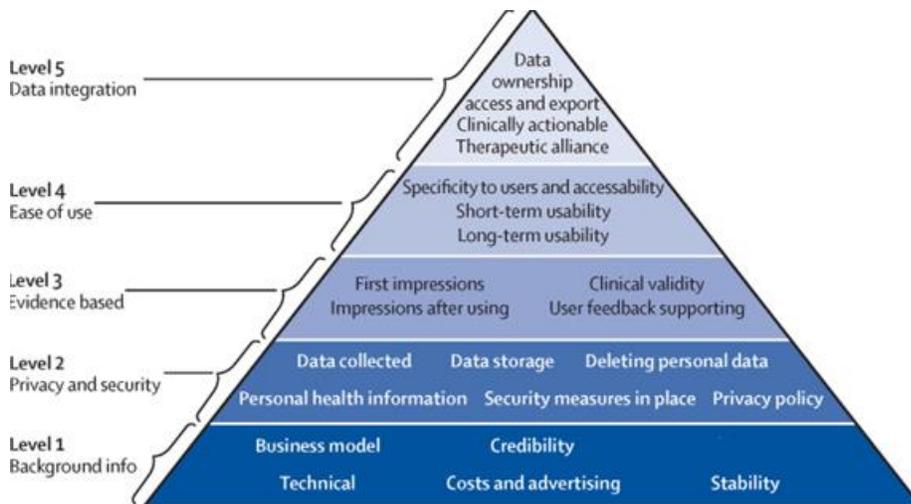
Public Safety App

In July 2019 the Brookline Police Department announced a public safety app to allow residents to make anonymous tips or crimes and suspicious activity. After comments and push back on the app, the Surveillance and Military Type Equipment Committee was asked to look into the application as well as look into more generally the method of using (mobile) apps. The above sections look at the later. Regarding the status of the actual public safety app, the company that produced it has dissolved and is no longer an ongoing entity and no information about the company or the app is available via the Internet. As a result, no further action is required concerning the specific application.

Corporations Division
Business Entity Summary

Request certificate	New search

Summary for: DEFENDDYNAMICS, INC.

The exact name of the Domestic Profit Corporation: DEFENDDYNAMICS, INC.	
Entity type: Domestic Profit Corporation	
Identification Number: 001362789	
Date of Organization in Massachusetts: 01-08-2019	
Date of Voluntary Dissolution: 05-11-2020	**Last date certain:**

References

1. Deriving a practical framework for the evaluation of health apps
2. Evaluation of a Mobile Phone App for Providing Adolescents With Sexual and Reproductive Health Information, New York City, 2013-2016
3. Mobile Application Tool Testing (National Institute of Standards and Technology (NIST)
4. SP 800-163 Rev. 1 Vetting the Security of Mobile Applications
5. A Risk Management Approach to Smart City Cybersecurity and Privacy