



NNEEDV

Co-parenting and Visitation Apps Review Checklist


This checklist is a part of a set of resources to help organizations evaluate co-parenting and visitation apps. We encourage you to start with the “Considerations for Judges and Supervised Visitation Providers: Co-parenting and Visitation Apps” resource before using this checklist to review a specific app.


App Name: _____

Privacy Policy	An app’s privacy policy should address the app directly, be readily available, and clearly communicate how user information is collected, stored, and shared.	<input checked="" type="checkbox"/>
Available on Website		
Clearly Written		
Scope is Specific to App [1]		
Policy Discusses:		
• Device Permissions Required		
• Data Collection & Retention		

[1] Sometimes privacy policies and terms of service are quite generic, and as a result, quite vague. The policy/terms should clearly have been developed for the app itself rather than copied wholesale from a template. If the company provides many products, it should be clear how the policy/terms apply to the specific product you are considering.


• Data Ownership		
• Secondary Data Use		


Terms of Service	An app's terms of service should address the app directly, be readily available, and clearly communicate the expected behavior of the user and business owner related to the app and its services.	
Available on Website		
Clearly Written		
Scope is Specific to App [1]		

Permissions	An app will request or require certain device access permissions from a user in order to carry out its functions. These requests should be clear in regards to whether information is required for functionality and how that information will be used. If too many permissions are required for functionality, they may interfere with a survivor's safety planning steps.	
Requested / Required		

Location		
Camera		
Microphone		
Contacts		
Phone		

Media Sharing	Apps are often used to share media (such as photos or videos), and it is important to know how media is protected in transit and how long its stored in the app.	<input checked="" type="checkbox"/>
Metadata (Does the app remove it from uploaded files?)		
Retention (Does the app delete stored images/videos after a certain period of time? What period of time?)		

User Data	Apps collect data in line with their privacy policy. It's important to consider what data is being collected, how it's protected in the app, how long it's stored, and who controls the length of time it is stored.	
Types Collected		
Encryption		
Storage		
Control (Can it be deleted after a period of time?)		

Web Portal	If an app offers web-based access, a web browser can create different security vulnerabilities for a survivor to consider, including the potential for third-party tracking. If a user logs into the app using a browser, does the app send data about the user to other companies (e.g. social media companies)? [2]	
Third-Party Tracking		

[2] [This article and chart of data sharing by telehealth startups](#) illustrates the kinds of data and companies being referred to. [Blacklight](#) is a web-based tool that can help identify tracking technologies embedded in a website and where they are sending user data .

Data Access	In addition to knowing what information is collected and stored, it's important to know who has access to what data within the app.	<input checked="" type="checkbox"/>
Parent's Own Data		
Other Parent's Data		
Children's Data		
Visitation Supervisor		
Court		
Tech Company [3]		

Financial Aspects	These apps cost money. It's important to consider how to make the app financially sustainable for the users.	<input checked="" type="checkbox"/>
Pricing		

[3] As a best practice, the tech company should not be able to access the data. This relates to the "encryption" item, in that encryption is required for this best practice. However, "encryption" with no other details is not sufficient to establish this, as there are different kinds of encryption. Companies should be specifically asked about their own access to user data.

Payment Processor		
--------------------------	--	--

Technical Analysis	It's important that the app meet the needs of the organization choosing it and the co-parenting families they work with, both in security and functionality.	<input checked="" type="checkbox"/>
Web Portal Security		
Functionality and User-Friendliness		

© 2024 National Network to End Domestic Violence, Safety Net Project. This project was supported by Grant No. [15JOVW-23-GK-05144-MUMU](#) awarded by the Office on Violence Against Women, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the Department of Justice, Office on Violence Against Women.