2023 International Client Seminar

March 2-5, 2023

MOBILE APPLICATIONS, SOCIAL MEDIA ADVERTISING AND THE INTERNET OF THINGS:

What's Your Appetite for Risk

JACOB LEHMAN
GERMAN, GALLAGHER, MURTAGH P.C.
Philadelphia, PA
lehmanj@ggmfirm.com

For better or worse, in modern society more and more of social and business interaction is conducted through our cell phones. While we may cringe when looking at data about how many times we pick up and look at our phones each day, or how much time we spend on social media, as business people and legal professionals it is important to recognize how this digital interface drives business and the legal challenges it presents.

Mobile applications are and seem destined to remain one of the central ways business is conducted. Companies developing an app for their business would be wise to consider the legal issues involved at every step of the app development process.

Legal Issues & App Development

Confidentiality Agreements - The first step in the mobile application development process usually involves retention of a software house to develop the mobile app. Development of the app inherently involves the use of confidential and proprietary business data of the company which can range from customer lists, to design technology to perhaps the product idea itself. Accordingly, the business ought to enter into a Non-Disclosure Agreement (NDA) to protect its information. This NDA should include all information concerning the business: financial data, know-how, show-how, operating, marketing, or trade data. Additionally, the definition should include information concerning the product: ideas, solutions, operating methods, functionalities, and elements of the app's architecture. Consider also, the obligations of the software house. They should include, among others, maintaining the confidentiality of all obtained confidential information, as well as an obligation according to which the other party will disclose information to its staff only if it is necessary and that it will obligate the staff to also maintain the secrecy of this information. As with any contract, for the NDA, choice of law provisions and enforcement clauses will also require close consideration.

Intellectual Property- Retention of a software house for app development also involves issues of intellectual property. Intellectual property (IP) relates to all work that is original and created during the mobile app development process. During the app development process, the business will be creating legal app ideas, original content, designs, logo, app names, source code, etc. All these original elements are considered IP and belong to the business. The company needs to register them as trademarks, copyright, or patents to protect the app idea.

Terms of Use - is a legal agreement that mobile app developers enter with their app's users. The agreement is valid automatically as soon as the user downloads the app. It states about the app, how the user must use it, what constitutes improper or unlawful use of the app and consequences of improper use. A Terms of Use agreement is crucial because it limits the possibility of legal and ethical issues for mobile apps if a user misuses the application or product.

EULA Agreements- Like terms of use, mobile applications almost always require an end user license agreement (EULA). All the major app stores require apps on their platform to have a EULA. The EULA is a contract between the owner of the app and the users using the app. It specifies the terms under which the end-user will use the app and identifies all permissible and non-permissible uses. The EULA will also ensure that the user isn't misusing the app in a harmful way. A EULA protects the intellectual property rights of software by outlining the specifics of what the user can and cannot do, or any other third party. Apart from identifying the business, the agreement also discloses the copyright license along with its terms and conditions relating to the app. With the EULA, the Developer can mitigate and alter liability for their website, define the permitted conducts and restrictions for their website, set up an indemnification process for your website and provide for incorporation an arbitration clause as deemed favorable.

In order for a EULA, or any terms and conditions to be effective, the user of the app needs to consent to these terms. The most effective way to get user consent is use of "clickwrap agreements''. Developers disclose them before the app is downloaded. The EULA is presented to the user, requiring them to state that they have read it and then agree to its terms by clicking on the "I Accept" button.

App Store Requirements- Once the app is ready, the next step is distribution of mobile apps through app stores. The app must comply with all app publishing requirements arising from the guidelines of Google and the guidelines of Apple. The developing business must also check government regulations for apps before distributing them. The terms and policies put emphasis on personal data protection and address IP issues concerning the app. These platforms also reserve the right to modify their legal terms or add new clauses when necessary. The app must comply with changes or else it will result in legal action or removal from the app store.

Privacy Laws and Mobile Applications

Almost all mobile applications are going to collect information from users. The web of laws that govern privacy of information shared online and collected by mobile applications is extensive. Depending on the jurisdiction in which the app is available, the type of information collected, and the intended users, multiple overlapping laws will apply. The best way to address this challenge is through a robust Privacy Policy that is reflective of how the company will gather, stores and share user data. Every situation is different but a summary of some of the relevant law is below:

FTC Regulations: For App Developers that intend to do business in the U.S., which will be most of them, The Federal Trade Commission has broad authority to regulate and enforce privacy under Section 5 of the Federal Trade Commission Act (FTC Act), which prohibits unfair or deceptive acts or practices in commerce. The FTC has issued various guidance documents addressing privacy and data security issues in the mobile app context. Notable for App Developers, the FTC recommends that mobile applications that collect personal information from users

- Create a privacy policy and make the policy available through the app stores (e.g., by posting the policy or a link to the policy on the app promotion page).
- Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information such as geolocation, financial, health, or children's data (to the extent platforms have not already provided such disclosures and obtained such consent).
- Coordinate and communicate with ad networks and other third parties (such as analytics companies) that provide services for apps so that accurate disclosures can be made to consumers.
- Participate in self-regulatory programs, trade associations, and industry organizations, which can provide guidance on how to make uniform, short-form privacy disclosures.

Additional information on FTC guidance is available at https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers

Children's Online Privacy Protection Act COPPA. The Children's Online Privacy Protection Act (COPPA)46 regulates the collection and use of personally identifiable information (PII) of children under the age of 13. The FTC is the primary agency that enforces COPPA and has issued implementing regulations, known as the COPPA Rule. The FTC has confirmed that the language of COPPA is broad enough to apply to mobile apps. Specifically, the agency has held that it views mobile apps as "online services" covered by COPPA because they "send and/or receive information over the Internet." The FTC has also issued guidance on privacy disclosures in kids' mobile apps.

HIPPA - A mobile app is subject to HIPAA if: The owner or operator of the app is a covered entity or business

associate. The app collects and/or stores protected health information (PHI). Covered entities are health care providers that conduct certain electronic transactions, health plans, and health care clearinghouses. Business associates are persons or entities that perform certain functions, activities, or services for or on behalf of a covered entity that involve the creation, receipt, maintenance, or transmission of PHI (such as claims processing, billing, and data analysis). If the mobile application collects or transmits individually identifiable health information in any form it is vital that HIPPA compliance be ensured.

Other Federal Laws that Mobile App Developers, should consider depending on the sector of the application include: Gramm-Leach-Bliley Act (GLBA)—financial products or services, Fair Credit Reporting Act (FCRA)—consumer credit reports, Video Privacy Protection Act (VPPA)—videotape service providers (including providers of online video streaming)

State Privacy Laws- If matters weren't complicated enough with the web of federal rules and regulations, states also have stepped into space of privacy legislation. The biggest is the California Consumer Privacy Act (CCPA). CCPA is a state law that establishes how business (including digital businesses) operating in CA, must handle the personally identifiable information of California residents. Notably, you must create a cookie policy that explains how your app collects and stores cookies and how third parties may use them. The California Privacy Rights Act (CPRA) is an addendum to the CCPA. It affects the notice and privacy requirements for apps that may be accessible to California consumers. The CPRA builds on the CCPA by requiring mobile apps that share personal data to comply with all relevant privacy laws. The California Online Privacy Protection Act (CalOPPA) applies to your app if it's located in California or serves California residents. You must use the word "privacy" when linking to your privacy policy from your app's homepage. You also need to put the last effective date of your privacy policy at the top of your privacy policy page, so users know which version of your policy they're reading.

California isn't the only entrant into this space. Illinois has enacted its own privacy law, the Biometric Information Privacy Act (BIPA) which currently is one of the toughest laws in the U.S. concerning the protection of biometric data. Under BIPA, any company doing business in Illinois or providing a service to Illinois residents that involves the collection of biometric data, must, obtain informed consent, may only disclose the data under limited circumstances, must adhere to retention and protection guidelines, and may not profit from the data. And under BIPA, biometric data is not limited to that collected by health or fitness apps. Courts have held that under BIPA, biometrics also includes, face, hand, retina or ear features. Similarly protected are behavioral characteristics including gestures, voice, typing rhythm, and gait. As such, any application using face ID or fingerprint for app. security would qualify. Any timekeeping or HR application would qualify. Of course any health and fitness application would qualify. BIPA contains a private right of action and a statutory damage of at least $1,000 for each violation.

Other states with their own privacy laws include Colorado, Utah, Virginia and Connecticut. Each of these statutes contain their own provisions regarding rights to access data, delete data, correct data and opt out of data collection.

GDPR- If your app offers services or goods to users in the EU, Norway, the UK, Switzerland, Iceland, or Liechtenstein, you must comply with the GDPR. You must create a privacy policy that establishes how, when, and where your app collects data.

Enforcement Actions- Failure to adhere to relevant privacy laws can lead to enforcement actions. Consider for example Snapchat, Inc. (photo messaging app—deceptive representations about the disappearing nature of messages sent through the app, the amount of personal data collected, the collection of geolocation

information, and security measures); and Goldenshores Techs., Inc. (flashlight app—failed to adequately disclose that precise geolocation and persistent device identifiers were transmitted to various third parties, including advertising networks, when users ran the app, and misrepresented how much control users had over the collection and use of their data).

Security failures or misrepresentations about the security available to users of the app. also has led to enforcement actions. Consider for example, Fandango, Inc. (movie ticketing app—deceptive representations about security when, among other things, the developer overrode default SSL certificate validation settings without implementing other security measures).

National Telecommunications & Information Administration (NTIA). NTIA is an agency of the U.S. Department of Commerce that serves as the President's principal adviser on telecommunications and information policy. It developed a voluntary code of conduct. The FTC has indicated that, for purposes of enforcement actions, it will look favorably on companies that adhere to NTIA's code of conduct.