FDA & FTC Regulation of Mobile Medical Apps

Michael D. Holloway
Institute for Science, Law & Technology
IIT Chicago-Kent College of Law
April 4, 2014

Smartphones and other mobile devices are playing an increasingly significant role in the way we live. Along with the dramatic expansion of these devices has come the development of a multitude of specialized software applications, or “apps,” for myriad purposes. Whether we want to order takeout, find a date, or figure out how to shake a head cold, there is a mobile app that can help us. Federal agencies, including the Food and Drug Administration (FDA) and Federal Trade Commission (FTC) are responding to rapid advances in mobile technology by identifying their unique benefits and risks and creating specialized regulatory frameworks to address the unique issues they raise. Mobile medical apps fall under the FDA’s regulatory umbrella to the extent that they constitute medical devices within the meaning of the Federal Food, Drug and Cosmetic Act. The FDA is primarily concerned with ensuring that mobile medical apps are safe. Mobile medical apps may also come under FTC scrutiny if their developers make unsubstantiated claims about their effectiveness or engage in deceptive or unfair practices in collecting or sharing users’ personal data.

Background – Prevalence of Smartphones and Mobile Apps

In June 2013, the Pew Research Center’s Internet & American Life Project reported that 91% of American adults owned a cell phone. Pew also reported that 61% of these, or 56% of all American adults, owned smartphones. In September 2013, Pew reported that 63% of cell phone owners use their phones to go online, with 34% mostly using their phones to access the internet, as opposed to a desktop computer, tablet, or other device. Additionally, 37% of teens ages 12-17 have smartphones, and three in four teens access the internet on mobile devices. A 2010 Research2Guidance study projected that by 2015, 500 million smartphone users worldwide will be using a mobile health app. Pew also reported in December 2013 that over half of smartphone owners get health information on their phones, and nearly one-fifth have downloaded health apps.

Advertisers are increasingly focusing on mobile devices as more people use them to connect to the internet. In November 2011, TechCrunch reported that by 2016, revenues from mobile health apps could be as high as $400 million, compared with $120 million as recently as 2010. In December 2012, VentureBeat reported that 80% of the top 50 U.S. ad buyers planned to increase their budget for mobile ads in 2013 and early 2014. Mobile ads accounted for 53% of Facebook’s revenue growth in the fourth quarter of 2013, compared with 23% in the fourth quarter of 2012.

Despite the increasing use of smartphones and other mobile devices, there is evidence that consumers have substantial concerns over privacy and the security of their personal information on these devices, and that app developers have not paid sufficient attention to privacy concerns. According to a 2011 report, only 19% of the top 340 free mobile apps linked to a written privacy policy. Fewer than one-third of respondents in a 2011 survey of U.S. smartphone users felt in control of their personal information on mobile devices. According to a December 2012 Federal Trade Commission report on mobile apps for kids, while nearly 60% of reviewed apps transmitted the device ID to a third party, and some transferred additional
information such as geolocation information or phone numbers, only 20% of the apps had an accessible privacy policy disclosing what information was shared.\textsuperscript{16} The FTC also reported in 2013 that 57% of mobile app users had either uninstalled or declined to install an app because they were concerned about sharing personal information.\textsuperscript{17}

\textbf{Food and Drug Administration (FDA)}

The Food and Drug Administration has the authority to regulate mobile medical apps that constitute medical devices under Section 201(h) of the Federal Food, Drug and Cosmetic Act, 21 U.S.C. § 321(h). The FDA is authorized to exercise oversight by requiring premarket approval of some devices.\textsuperscript{18} The FDA also conducts postmarket surveillance of medical devices\textsuperscript{19} and is authorized to order the recall of noncompliant devices.\textsuperscript{20}

Section 201(h) of the Food, Drug and Cosmetic Act, 21 U.S.C. § 321(h), defines a “device” as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is

\begin{enumerate}
\item[(1)] recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,
\item[(2)] intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
\item[(3)] intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.”\textsuperscript{21}
\end{enumerate}

The intended use of a device is determined on the basis of “labeling claims, advertising materials, or oral or written statements by manufacturers or their representatives. When the intended use of a mobile app is for the diagnosis of disease or other conditions, or the cure, mitigation, treatment, or prevention of disease, or is intended to affect the structure or any function of the body of man, the mobile app is a device.”\textsuperscript{22} For example, an app using a light-emitting diode (LED) to illuminate objects generally would not be considered a medical device.\textsuperscript{23} If, however, the same app was promoted by its manufacturer through marketing, labeling, and the circumstances surrounding its distribution for use by doctors as a light source for examining patients, the app would be considered a medical device falling within the FDA’s authority.\textsuperscript{24}

On September 25, 2013, the FDA issued a final guidance on mobile medical apps, defined as those mobile apps\textsuperscript{25} that meet the definition of device in Section 201(h), and which are intended either:

\begin{itemize}
\item “to be used as an accessory to a regulated medical device, or
\item to transform a mobile platform into a regulated medical device.”\textsuperscript{26}
\end{itemize}

For example, the guidance describes, as examples of devices falling within the FDA’s regulatory focus, mobile “apps that provide the ability to control inflation and deflation of a blood pressure cuff through a mobile platform and mobile apps that control the delivery of insulin on an insulin pump by transmitting control signals to the pumps from the mobile platform.”\textsuperscript{27} These are examples of apps to be used as accessories to regulated medical devices. The guidance also gives examples of mobile apps used to transform a mobile platform into a regulated device, such as “attachment of a blood glucose strip reader to a mobile platform to function as a glucose
Like all medical devices subject to FDA regulation, a mobile medical app may be classified as Class I (low risk), Class II (medium risk), or Class III (high risk). Manufacturers of medical devices are required to register with the FDA, to provide a list of devices they market, and to provide premarket submissions as applicable, based on device classifications. A medical device manufacturer can determine the proper classification of a medical device by searching the Product Classification section of the FDA website to determine the name, class number, and federal regulation number for a given device, as well as whether it is exempt from further premarket notification or approval requirements.

In a November 2013 survey, the mobile health news website mobihealthnews.com found 103 mobile medical apps registered with or cleared by the FDA as medical devices. Only one of these, a device allowing previously approved electrocardiogram software to be linked to a handheld personal digital assistant, was a Class III device requiring premarket approval by the FDA.

In its guidance, the FDA has specified categories of mobile medical apps which it intends to make the focus of its regulatory oversight. These include all mobile apps “that are an extension of one or more medical devices by connecting to such device(s) for purposes of controlling the device(s) or displaying, storing, analyzing, or transmitting patient-specific medical device data”; those “that transform the mobile platform into a regulated medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices”; and those “that become a regulated medical device (software) by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations.”

For apps that meet the definition of medical devices but which the FDA determines pose a lower risk to the public, the FDA “intends to exercise enforcement discretion (meaning it will not enforce requirements under the FD&C Act).” Rather, “the FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient’s safety if the mobile app were to not function as intended.” Jeffrey Shuren, MD, director of the FDA’s Center for Devices and Radiological Health, stated, “Although many mobile apps pertain to health, we are only continuing our oversight for a very small subset of those mobile apps that are medical devices.”

The FDA has identified several categories of mobile apps for which it intends to exercise “enforcement discretion.” The FDA does not intend to regulate apps “that provide or facilitate supplemental clinical care, by coaching or prompting, to help patients manage their health in their daily environment.” For example, the FDA will exercise enforcement discretion with respect to apps that use features like video games to motivate users to do physical therapy exercises at home. Similarly, the FDA does not intend to regulate apps “that provide patients with simple tools to organize and track their health information,” such as apps that provide reminders or tracking tools for patients with gum disease. The FDA does not intend to regulate “apps that provide easy access to information related to patients’ health conditions or treatments (beyond providing an electronic ‘copy’ of a medical reference)”; “apps that are specifically marketed to help patients document, show, or communicate to providers potential medical conditions”; or “apps that perform simple calculations routinely used in clinical practice,” such as body mass index or APGAR score (a common measure for assessing the health of
newborns). Finally, the FDA does not intend to regulate apps that provide patients and providers with mobile access to health record systems.

One example of a medical app falling within the FDA’s regulatory focus is eMotion ECG Mobile, an ECG monitor that connects to Android smartphones for continuous ECG monitoring. In December 2013, ECG Mobile was approved by the FDA as a Class II medical device. The device competes with AliveCor, another smartphone-connected ECG monitor approved by the FDA. ECG Mobile is a device prescribed by a doctor and worn by a patient under his or her clothing. ECG readings are continuously sent to the patient’s Android phone, and from there, to a server from which the clinician can access them via a web browser. It also sends the clinician an alarm in the case of irregular heart rate readings. Users can also enable a GPS feature intended to allow first responders to find them more easily in case of emergency. Unlike AliveCor, ECG Mobile enables continuous rather than sporadic ECG monitoring on a smartphone, the first mobile app to do so.

In addition to its premarket approval process, the FDA undertakes postmarket surveillance to ensure medical device safety and performance. The FDA defines “postmarket surveillance” as “the systematic collection, analysis, interpretation, and dissemination of health-related data to improve public health and reduce morbidity and mortality.” It does this through a system of adverse event reporting, postmarket studies, and other tools such as recalls and enforcement actions.

In September 2012, the FDA issued a report, Strengthening our National System of Medical Device Postmarket Surveillance, in which it laid out its current framework for conducting postmarket surveillance. The postmarket surveillance program is intended to “quickly identify poorly performing devices, accurately characterize and disseminate information about real-world device performance, including the clinical benefits and risks of marketed devices, and efficiently generate data to support premarket clearance or approval of new devices and new uses of currently marketed devices.” In its report, the FDA outlined a vision including “the creation of a national system that conducts active surveillance in near real-time using routinely collected electronic health information containing unique device identifiers, quickly identifies poorly performing devices, accurately characterizes the real-world clinical benefits and risks of marketed devices, and facilitates the development of new devices and new uses of existing devices through evidence generation, synthesis and appraisal.” The report noted specifically that medical device postmarket surveillance should:

- “Provide timely, accurate, systematic, and prioritized assessments of the benefits and risks of medical devices throughout their marketed life using high quality, standardized, structured, electronic health-related data;
- Identify potential safety signals in near real-time from a variety of privacy-protected data sources;
- Reduce burdens and costs of medical device postmarket surveillance; and,
- Facilitate the clearance and approval of new devices, or new uses for existing devices.”

To these ends, the report proposed four specific actions:
1. “Establish a Unique Device Identification System and Promote Its Incorporation into Electronic Health Information;

2. Promote the Development of National and International Device Registries for Selected Products;

3. Modernize Adverse Event Reporting and Analysis; and

4. Develop and Use New Methods for Evidence Generation, Synthesis and Appraisal.”

In April 2013, the FDA issued an update to the report that incorporated stakeholder input and specified a timeline for next steps. The FDA has taken postmarket enforcement action with regard to a mobile medical app intended for consumer use. In May 2013, the FDA issued a letter notifying Biosense Technologies Private Limited that its uChek urine analysis app constituted a medical device under Section 210(h) requiring FDA clearance. uChek used a smartphone’s camera to analyze urinalysis dipsticks and reported the results to the user. While the urinalysis strips analyzed by the app had been cleared by the FDA for interpretation by visual inspection, the FDA found that uChek transformed the smartphone into a medical device by functioning as an automated strip reader. Thus, uChek was a medical device requiring separate FDA clearance. The letter directed Biosense to the 510(k) Substantial Equivalence Determination for the Mission U500 Urine Analyzer, a similar automated strip reading system, as an example of a cleared device. In a later interview, Biosense CEO Myshkin Ingawale stated that Biosense had resolved the issues with the FDA by offering on the market only a limited version of uChek that qualified as a 510(k)-exempt Class I device, and initiating the compliance process for uChek Universal, a full version qualifying as a Class II device requiring premarket clearance.

**Federal Trade Commission (FTC)**

The FTC is directed, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, to prevent “unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce.” These include any act or practice which “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” 15 U.S.C. § 52 defines false advertisements as unfair or deceptive acts or practices falling within the scope of the FTC’s enforcement authority. In addition to this enforcement authority, the FTC has a Mobile Technology Unit that performs research, marketplace monitoring, and internal staff training on issues related to mobile devices.

The FTC has taken steps to educate businesses and consumers on the privacy concerns surrounding commerce on mobile devices. In May 2012, the FTC hosted a mobile privacy panel discussion, “In Short: Advertising and Privacy Closures in a Digital World,” which included representatives from industry, trade associations, academia, and consumer privacy groups to explore privacy disclosures on mobile devices. In December 2012, the FTC released a staff report, *Mobile Apps for Kids: Disclosures Still Not Making the Grade*, examining the privacy disclosures and practices of children’s apps. In February 2013, the FTC released a report, *Mobile Privacy Disclosures: Building Trust Through Transparency*, which set forth recommended privacy practices for mobile app developers and consumers. Also in February
2013, the FTC released an online business guide, “Mobile App Developers: Start with Security,” which “encourages developers to aim for reasonable data security, evaluate the app ecosystem before development, and includes tips such as making someone responsible for data security and taking stock of the data collected and maintained.”

Another FTC business guide, “Marketing Your Mobile App: Get it Right From the Start,” discusses truth in advertising and respect for user privacy.

In addition to its efforts to educate consumers and developers, the FTC has taken enforcement actions against mobile medical app developers for making unwarranted claims of efficacy. In September 2011, the FTC announced settlements with the makers of two purported acne treatment apps, AcneApp and Acne Pwner. Both apps claimed to treat acne by emitting colored lights. The apps directed users to hold the screen next to the area of skin to be treated while the app was activated. Acne Pwner, which sold for 99 cents and had approximately 3,300 downloads, advertised, “Kill ACNE with this simple, yet powerful tool!” According to the FTC, the makers of AcneApp, which sold for $1.99 and had approximately 11,600 downloads, made a misleading claim that a British Journal of Dermatology study had proven blue and red light therapy of the kind AcneApp provided to be effective in treating acne. The FTC filed complaints against both app developers, alleging that these misrepresentations constituted unfair or deceptive acts or practices in violation of 15 U.S.C. § 45, and false advertisements in violation of 15 U.S.C. § 52. The actions resulted in settlements barring AcneApp and Acne Pwner from “making acne-treatment claims about their mobile apps and other medical devices, or claims about the safety, performance, benefits, or efficacy of any device unless they have scientific evidence.” The makers of AcneApp were further “barred from misrepresenting research, tests, or studies.” The makers of AcneApp were fined $14,294, and the maker of Acne Pwner was fined $1,700.

The FTC has also taken enforcement action against other mobile app developers that were not offering medical apps. These actions nevertheless shed light on the types of privacy and disclosure standards that medical apps will need to meet. As its guidance publications and enforcement actions show, the FTC is particularly concerned with requiring mobile app developers to provide notice and obtain consent before collecting and sharing users’ personal and location information. The FTC also enforces the Children’s Online Privacy Protection Rule (“COPPA Rule”), which prohibits mobile apps and other online services from collecting personal information from children under 13 without parental consent.

In August 2011, the FTC announced a settlement with W3 Innovations, LLC, doing business as Broken Thumbs Apps. W3 developed several apps marketed to children, including Emily’s Girl World, Emily’s Dress Up, Emily’s Dress Up & Shop, and Emily’s Runway High Fashion, and listed them in the “Games—Kids” section of Apple’s App Store. The apps, which had over 50,000 downloads, allowed users to play games, create virtual models, and design outfits. Users were encouraged to email “Emily” and to email comments to “Emily’s Blog.” According to the FTC, W3 collected and maintained thousands of email addresses from app users in this way. The apps also allowed children to post information, including personal information, via online message boards. The FTC alleged that W3 violated the COPPA Rule by failing to disclose its information-collection practices or obtain verifiable parental consent before collecting or disclosing personal information from children. W3 paid $50,000 to settle the charges.

In October 2011, the FTC reached a settlement with Frostwire, a peer-to-peer file sharing software developer offering a file sharing app for Android mobile devices. According to the
FTC, “Frostwire had configured the application’s default settings so that, immediately upon installation and set-up, it would publicly share users’ photos, videos, documents, and other files stored on those devices.” The FTC alleged that “little or no notice was provided to [the] user at the time the files [were] shared.” The FTC alleged that Frostwire’s file sharing app was unlawful because it misrepresented how downloaded files were shared, and because its unfair design was likely to cause a significant number of consumers to unwittingly share files stored on their mobile devices. The resulting settlement barred Frostwire from “using default settings likely to cause inadvertent public sharing of files by consumers” and required “clear and prominent disclosures about file sharing and how to disable it.” Frostwire was further barred from making substantial misrepresentations about its software’s file-sharing behavior.

In February 2013, the FTC announced a settlement with Path, Inc., makers of the mobile social networking app Path, over its collection of user data. In its press release, the FTC described Path as “a social networking service that allows users to keep journals about ‘moments’ in their life and to share that journal with a network of up to 150 friends.” Path allowed users to “upload, store, and share photos, written ‘thoughts,’ the user’s location, and the names of songs to which the user is listening.” The FTC alleged that Path collected personal information from users’ mobile device address books without their knowledge or consent. Specifically, the complaint alleged that the user interface was misleading, and that it provided users with no meaningful choice about whether user data would be collected. The app collected and stored information from the user’s mobile device address book even if the user did not elect to find friends using this stored contact information. The FTC also alleged that Path’s privacy policy deceived consumers by claiming that it automatically collected only certain user information such as IP address, operating system, browser type, address of referring site, and site activity information, when in fact version 2.0 for iOS automatically collected and stored address book data at first launch and each time the user signed in. Additionally, the FTC alleged that Path violated the COPPA Rule by collecting personal information from approximately 3,000 children under age 13 without parental consent. The settlement required Path to establish a comprehensive privacy program and to obtain independent privacy assessments every other year for 20 years. Path also paid $800,000 to settle the COPPA charges.

Along similar lines, in December 2013, the FTC announced a proposed settlement with Goldenshores Technologies, LLC, the maker of Brightest Flashlight Free, an Android app with tens of millions of downloads, over its undisclosed collection and sharing of users’ geolocation information. According to the FTC, the app’s privacy policy “deceptively failed to disclose that the app transmitted users’ precise location and unique device identifier to third parties, including advertising networks.” Furthermore, the app began collecting and transmitting location data and the unique device identifier even before the user could accept or reject the end-user license agreement. The proposed settlement “prohibits [Goldenshores] from misrepresenting how consumers’ information is collected and shared and how much control consumers have over the way their information is used.” The proposed settlement also requires Goldenshores to “provide a just-in-time disclosure that fully informs consumers when, how, and why their geolocation information is being collected, used and shared,” and to obtain affirmative, express consent before information is collected.

In sum, the agency guidance the FTC has issued and the enforcement actions it has taken against app developers to date show that the agency is focused closely on issues of truth in advertising and data privacy that frequently come into play with respect to mobile medical apps.
For the definition of “device,” see § 201(h) of the Food, Drug and Cosmetic Act, 21 U.S.C. § 321(h).


3 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, Food and Drug Administration, Sept. 25, 2013, p. 13 (“FDA intends to apply its regulatory oversight to only those mobile apps that are medical devices and whose functionality could pose a risk to a patient’s safety if the mobile app were to not function as intended.”)


20 21 U.S.C. § 360h(e); 21 C.F.R. § 810.1 et seq.


22 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, Food and Drug Administration, Sept. 25, 2013, p. 8 (citing 21 C.F.R. § 801.4).

The FDA defines a “mobile app,” for purposes of the guidance, as “a software application that can be executed (run) on a mobile platform (i.e., a handheld commercial off-the-shelf computing platform, with or without wireless connectivity), or a web-based software application that is tailored to a mobile platform but is executed on a server.” Examples of “mobile platforms” include “mobile computers such as smart phones, tablet computers, or other portable computers.”

---

34 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, Food and Drug Administration, Sept. 25, 2013, pp. 13-16 (internal citations omitted).
38 Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, Food and Drug Administration, Sept. 25, 2013, p. 16.


