MOBILE APPS: REDEFINING THE VIRTUAL CALIFORNIA ECONOMY AND THE LAWS THAT GOVERN IT

By Alexandra McDonald, Jason McDonell, and Caroline Mitchell[1]

I. INTRODUCTION.

As the virtual world integrates seamlessly into our everyday lives, mobile applications ("apps") have become a hub of both social and commercial activity. As a result, they have drawn increasing attention from courts and regulators. In California's Silicon Valley driven economy, savvy businesses closely monitor their apps portfolios, making sure they have the legal protections necessary to optimize their value, while also guarding against the legal and regulatory pitfalls that could plunge them into high profile and costly disputes. This article reviews the rapid rise of apps in the economy and the legal issues that companies using apps to drive their business need to manage.

II. THE NEW FACE OF CONSUMERISM.

The recent proliferation of mobile apps has rapidly changed the way consumers interact with businesses, and there are no signs that these changes will slow down. According to Statista.com, the global mobile app industry has grown from an $8 billion a year market in 2011, to a $45 billion market in 2015.[2] Statista.com projects that the industry will generate $76 billion, with an estimated 268 billion downloads, in 2017.[3] Mobile device sales and use are staggering: as of 2014, 91% percent of the U.S. adult population owned a cell phone, and 61% percent of those owned a smartphone.[4] Mobile devices now outsell personal computers by double and by 2016, mobile devices in use worldwide will exceed the number of people on the planet, with each person owning approximately 1.4 devices.[5] Similarly, mobile app availability and consumer use are on the rise. At the end of 2013, 57% of U.S. mobile users said they use their apps daily and, on average, mobile device owners each use 26.8 apps collectively for more than 30 hours per month, with users age 25 to 34 logging even more time on their apps.[6]

On any given day, the average mobile user could use an app to make a credit card payment, get a ride with a private driver, share photos on social media, chat with a potential date, purchase extra lives in their favorite game, sublet an apartment, track the number of steps taken throughout the day, trade stock, video chat with a doctor, and have dry cleaning delivered. It's no wonder we are used to hearing the catchphrase: "There's an app for that." Among the apps with the most usage by mobile app audiences are: Facebook, reaching

---

1 Caroline Mitchell is a partner in the Global Disputes practice, Jason McDonell is a partner in the Business and Tort Litigation practice, and Alexandra McDonald is an associate in the Cybersecurity, Privacy and Data Protection practice in the San Francisco office of Jones Day. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the law firm with which they are associated.

2 *Worldwide mobile app revenues from 2011 to 2017 (in billion U.S. dollars),* STATISTA.COM, http://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/ (last visited August 3, 2015).

3 *Id.*

4 *The Future of Mobile Application Development,* ENTREPRENEUR.COM, http://assets.entrepreneur.com/article/1409068924-by-2017-app-market-will-be-77-billion-dollar-industry-infographic.jpg (last visited August 3, 2015).

5 *Id.* One billion mobile devices are expected to be sold in 2015.

6 *Id.*

74% of users per month; Google Play, Google Search, and YouTube, reaching around 50%; and Pandora, Google Mail and Maps, Instagram, and Twitter, reaching roughly 30 to 45% of user per month.[7] Notably, as of mid-2014, there were 399 million Facebook users who accessed the site exclusively through a mobile device.[8] In terms of availability on Apple's App Store, games account for over 20% of available apps, with education, business, entertainment, and lifestyle apps following.[9]

California is at the epicenter of this revolution in how consumers use mobile devices and the economic and legal issues that come with it. As of July 2015, the California-based Google Play Store and Apple App Store had 1.6 million and 1.5 million apps available for download, respectively.[10] Google and Apple each offer about twice as many apps as Amazon, Windows, and BlackBerry combined.[11]

While most apps are offered at little or no cost, they are able to generate tremendous amounts of revenue. They do so in five ways: by charging to download the app; by promoting advertisements; by offering in-app purchases; by completing purchases of out-of-app goods and services; and by selling the user data they collect. "In-app purchases" or IAPs are purchases of a virtual good delivered within an app—like virtual coins in the Bejeweled app or a Kindle e-book delivered via the Kindle app to your iPhone.[12] This is in contrast to a purchase of a tangible good or service external to an app, like a pair of shoes purchased within the Nike app or an Uber ride.[13] The majority of apps in which IAPs take place are initially free to download but allow access to premium content at a price, earning these apps the moniker "freemium."[14] But don't let the word "free" fool you: in 2012, global revenue from mobile IAPs was $2.11 billion, with future growth projected at

---

7 To view percentage of users reached as of September 2013, see *Mobile App Usage,* Forbes.com, http://blogs-images.forbes.com/niallmccarthy/files/2014/10/Giant-social-apps_Forbes.jpg (last visited August 3, 2015). To view the number of unique monthly users as of 2013, see *Most popular mobile apps in the U.S. for iOS and Android,* Statista.com, http://www.statista.com/statistics/324922/top-mobile-apps-average-unique-users/ (last visited August 3, 2015)

8 *Mobile App Usage, supra* note 7.

9 Niall McCarthy, *Mobile App Usage By The Numbers [Infographic],* Forbes.com (October 29, 2014, 9:00 AM), http://www.forbes.com/sites/niallmccarthy/2014/10/29/mobile-app-usage-by-the-numbers-infographic/. *See also, Most popular Apple App Store categories in June 2015,* Statista.com, http://www.statista.com/statistics/270291/popular-categories-in-the-app-store/ (last visited August 3, 2015).

10 *Number of apps available in leading app stores as of July 2015,* Statista.com, http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (last visited August 3, 2015).

11 *Id.*

12 Forrest Stroud, *in-app purchase,* Webopedia, http://www.webopedia.com/TERM/I/in-app_purchase.html (last visited August 3, 2015). *See also,* Jay Yarow, *Amazon Has Found a Clever Way to Avoid Giving Apple a 30% Cut of eBook Sales—Here's How,* Business Insider (January 11, 2012, 11:30 AM), http://www.businessinsider.com/amazon-kindle-ipad-store-2012-1?op=1. Apple take a 30% cut of all "in-app purchases" delivered via an app to the iPhone. Amazon has skirted this IAP fee by delivering content through its store app or Kindle app to non-iPhone devices.

13 Oscar Waczynski, *How do apps like Lyft, Uber, AirBnB skirt Apple's 30% cut on each transaction?,* Designer News, https://www.designernews.co/stories/9695-how-do-apps-like-lyft-uber-airbnb-skirt-apples-30-cut-on-each-transaction (last visited August 3, 2015).

14 71% of in-app purchases take place in apps that are initially free to download. *See, In-app purchases from 'freemium' titles account for 71% of iPhone app revenue,* appleinsider.com (March 29, 2013, 08:58 AM), http://appleinsider.com/articles/13/03/29/in-app-purchases-from-freemium-titles-account-for-71-of-iphone-app-revenue.

$14 billion for 2015 and $35 billion for 2017.[15] IAPs—the majority of which take place in games—also generated ten times more revenue than advertising for games and substantially more than pre-paid games (meaning those games that a user pays to download on a mobile device or game console).[16]

But free and low cost apps do more than generate enormous revenue: the data they collect and store is, by itself, extremely valuable—generating an estimated $5.5 billion in revenue in 2013.[17] The ubiquitous availability and use of mobile apps has resulted in an unprecedented collection of rich, inter-connected consumer data. The emergence of the term "big data" refers to the omnipresent tracking of every digital process we undertake and apps play an essential role in this process.[18] Apps can access a mobile-device-user's contacts, text messages, photos and videos, credit card information, and even facial features. They can then combine user data with the mobile device's unique ID, wireless signals, and geolocation history to create a down-to-the-minute profile of any user, whether or not an app is open or in use.[19]

The app provider or distributor can then sell this layered and complex profile to third-party researchers and even companies and advertisers trying to target consumers. For example, Verizon's "Precision Market Insights"[20] collects and sells statistical data about the activities of mobile phone users in locations like malls, stadiums, and near billboards; Air Sage uses wireless signals from mobile phones to track consumer habits, such as movements of California commuters;[21] and Sprint, among many other companies, collects and sells aggregated and anonymized data of its mobile users for market research purposes.[22] As every detail of our lives become linked to Internet-connected devices and associated apps—from smartphones and fitness trackers to interconnected thermostats and self-driving cars—the data this "Internet of Things" will supply will become more and more valuable.[23]

With this new app-economy and the proliferation of "big data" come an array of legal issues, as the law tries to catch up with the new realities in the marketplace. Existing legal doctrines and regulations are just beginning to address these issues, which include consumer rights, contractual relationships, privacy, data protection, and regulated industries. As a result, the legal landscape related to apps is changing rapidly, and will continue to evolve as app use and the data generated from it grow exponentially.

---

15 *Total worldwide in-app purchase revenues from 2011 to 2017 (in million U.S. dollars),* Statista.com, http://www.statista.com/statistics/220186/total-global-in-app-revenue-forecast/ (last visited August 3, 2015).

16 Tero Kuittinen, *In-app purchases now dominate the portable game market,* BGR.com (June 13, 2013, 2:10 PM), http://bgr.com/2013/06/13/mobile-gaming-in-app-purchases-analysis/#.

17 *Mobile Operator Guide 2013, The Evolution of Mobile Services,* SAP Mobile Services, http://www.sap.com/bin/sapcom/el_gr/downloadasset.2013-02-feb-07-18.mobile-operator-guide-2013-pdf.html (last visited August 3, 2015).

18 *What is Big Data,* IBM, http://www.ibm.com/big-data/us/en/ (last visited August 3, 2015).

19 John Kennedy, *Reining In Mobile App Privacy Practices,* LAW360.com (January 25, 2013, 12:23 PM ET), www.law360.com/articles/407974.

20 Precision Market Insights From Verizon, http://precisionmarketinsights.com.

21 *See* airsage, www.airsage.com; *White Paper,* airsage, http://www.airsage.com/Contact-Us/White-Paper/.

22 *See* Sprint Corporation Privacy Policy, *available at* http://www.sprint.com/legal/privacy.html#contact.

23 *See* Philip Blum, *'Internet Of Things' 101: Legal Concerns,* LAW360.com (April 14, 2014, 11:51 AM ET), http://www.law360.com/articles/526266.

III. THE LEGAL FOUNDATION FOR APPS.

A. Creation and Distribution of Mobile Apps.

The mobile app ecosystem includes providers of hardware, software, and services. Mobile devices are manufactured by original equipment manufacturers (OEMs) such as Apple or Samsung. Content providers, like Facebook, create the apps using software development kits and related tools licensed from the owners of the major mobile operating systems (*e.g.* Apple's iOS, Google's Android, and Microsoft's Windows Phone).[24] Wireless telecommunications service providers, like Verizon Wireless and AT&T Mobility, operate the wireless networks necessary for mobile communications. The vast majority of apps are sold through a handful of distribution platforms:

COMPANY	PLATFORM	DATE OF ENTRY	AVAILABLE APPS[24]
Apple Computer	App Store	July 2008	1.5 million
Google Inc.	Google Play	October 2008	1.6 million
Amazon.com, Inc.	Amazon App Store	March 2011	360,000
Microsoft Corporation	Windows Store	February 2012	340,000

Layered on top of these elements, are providers of many specialized technologies and services that can be built into or linked to an app. These include advertising, measuring tools (such as Google Analytics for Mobile Apps, which measures the value of apps), cloud storage services, network messaging, monetization services, and payment systems.[26]

B. Contractual Building Blocks.

In bringing an app to market, there are important contracts entered into between (1) the app providers or developers and distributors; (2) the providers and end users; and (3) the distributors and end users. These agreements define and protect the parties' intellectual property rights and confidential information, establish basic commercial terms for the distribution, purchase and use of the apps, and provide for compliance with privacy and data security laws and policies.

---

24 Content providers are sometimes assisted by a growing industry of services providers. For example, Amazon Web Services (AWS) provides tools to create mobile apps, will manage the backend, so the content providers does not have to provision, scale, or monitor servers. *See Develop apps quickly. Scale, test and run reliably,* AWS MOBILE SERVICES, https://aws.amazon.com/mobile/?nc1=f_dr (last visited August 3, 2015).

25 *Number of apps available in leading app stores as of July 2015,* STATISTA.COM, http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ (last visited August 3, 2015).

26 These are just the basics of what is involved in creating a mobile app. In practice, an app development may include any or all of following: the handset OEM; the application programming interface (API) software development kit (SDK); a mobile services provider; an API manager; identity and access management (IAM) authorization controls; middleware; a database; security; a platform-as-a-service (PaaS) provider; *infra*structure-as-a-service (IaaS); a mobile enterprise application platform (MEAP); mobile device management (MDM); mobile application management (MAM); and other service providers of social media, location, and many others.

1. Agreements between App Providers or Developers and Operating System Distributors.

To create an app for a particular operating system, the developer must enter into agreements with the operating system owners/distributors to get access to the software development kits (SDKs) and related tools that are used to build the apps. Each of the major distributors has a standard developer license agreement for this purpose. In addition, the providers must accept the distributors' terms and conditions for making the apps available through the distributors' mobile stores.

Apple licenses its operating system to developers through its iOS Developer Program License Agreement.[27] This agreement governs the app provider's use of Apple software to develop iOS-compatible applications as well as the app's submission to and distribution on Apple's App Store. Google has separate agreements for development of the app using its Android software and distribution on the Google Play store. Google makes Android software available under the Android Open Source Project[28] and uses the Android Software Development Kit License Agreement[29] to license its SDK to Android-compatible app developers. Google's terms for distribution are set forth in its Google Play Developer Distribution Agreement.[30]

These agreements address compliance with privacy and other consumer protection laws. For example, Apple's iOS Development Program License Agreement provides that use of the app "must comply with all applicable privacy laws. . . ."[31] It provides that the app "may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising. . . ."[32] It further requires the app developer to "provide clear and complete information to users regarding Your collection, use and disclosure of user or device data, *e.g.,* a link to Your privacy policy on the App Store."[33] Also included are provisions concerning warranty and support of the app; non-disclosure of any information deemed confidential by the operating system owner; and indemnification of operating system owner from losses arising from breach, violation of intellectual or proprietary rights, and end-user claims regarding the provider's app.

2. Agreements between App Distribution Platforms and End-Users.

Each of the major distributors requires consumers to agree to the distributor's terms and conditions the first time the consumer accesses the store to download an app. The terms and conditions then control subsequent app downloads. The app distribution platforms include similar provisions in these end user agreements. Agreements from both Apple and Google cover

---

27 *iOS Developer Program License Agreement,* APPLE.COM, https://developer.apple.com/programs/terms/ios/standard/ios_program_standard_agreement_20140909.pdf (last visited August 3, 2015).

28 *Welcome to the Android Open Source Project!,* SOURCE.ANDROID.COM, https://source.android.com/ (last visited August 3, 2015).

29 *Terms and Conditions,* DEVELOPER.ANDROID.COM (November 13, 2012), https://developer.android.com/sdk/terms.html.

30 *Google Play Developer Distribution Agreement,* GOOGLE.COM (May 5, 2015), https://play.google.com/about/developer-distribution-agreement.html.

31 *See Id.* § 3.3.8.

32 *Id.* § 3.3.9.

33 *Id.* § 3.3.10.

payment and refund policies and various user restrictions.[34] For example, Apple's agreement provides that the user is "solely responsible . . . for all activities that occur on or through your account."[35] Furthermore, both agreements disclose that the distribution platform is acting as a marketing agent and that some content may have been developed by a third-party provider. In addition, the agreements include provisions concerning termination, limitation of liability, indemnification, and possible disclosure of personal information to law enforcement.

Agreements from Apple and Google incorporate by reference their respective privacy policies.[36] Privacy policies generally explain what information is collected, why and how it is used, and how it is protected. Collected information includes, but is not limited to: personal information such as names, contact information, and credit card numbers; device information such as a device's universally unique identifier (*e.g.* the IMEI of a mobile phone); and GPS location information. Furthermore, these policies include information about the disclosure and transfer of information to third-parties. These policies state that collected information is used to protect, maintain, improve upon, and develop services for users. Additionally, the distribution platforms disclose that they may make limited aggregate data available to third-party app providers on request to ensure improvement of products.

3. Agreements between App Providers and End Users.

App providers typically require end users to accept terms and conditions of use when they download the app. As an example, the photo sharing app Instagram's Terms of Use provide, among other things: a minimum age requirement (13 years); prohibitions on certain content (*e.g.*, "violent," "infringing," "hateful"); and that the user is responsible for their own conduct and posts to the site.[37] These agreements disclose privacy policies of the provider, and set forth other general legal provisions such as terms of warranty, termination, limitation of liability, severability, waiver and construction, export control, and dispute resolution.

IV. THE LEGAL LANDSCAPE.

A. Apps Enter the Courtroom and the Regulatory Arena.

In many ways, a mobile app is treated like any other internet-based business or website under the law. Consumers and private parties bring individual or class action lawsuits against app owners or distribution platforms for the harm suffered under private causes of action. Concomitantly, federal and state agencies and state Attorneys General may bring enforcement actions against app owners and distribution platforms for the violation of

---

34 *See Terms And Conditions,* Apple.com (June 30, 2015), http://www.apple.com/legal/internet-services/itunes/us/terms.html. *See also Google Play Terms of Service*, Google.com (December 10, 2014), https://play.google.com/intl/en_us/about/play-terms.html. *See also Amazon Appstore for Android Terms of Use,* Amazon.com (April 2, 2014), https://www.amazon.com/gp/help/customer/display.html?nodeId=201485660. *See also Microsoft Services Agreement*, Microsoft.com (August 14, 2013), http://windows.microsoft.com/en-us/windows/windows-store-terms-of-use.

35 *See Terms And Conditions,* Apple.com, *supra* note 34.

36 *Privacy Policy,* Apple.com, http://www.apple.com/legal/privacy/en-ww/ (last updated December 10, 2014). *See also, Welcome to the Google Privacy Policy,* Google.com, https://www.google.com/intl/en/policies/privacy/ (last updated June 30,215).

37 *Terms of Use,* Instagram.com (January 19, 2013), https://instagram.com/about/legal/terms/.

federal and state regulations. Special considerations arise for apps related to the new ways in which consumers are able to interface with businesses, the ease with which apps may collect rich and often unexpected consumer data, and the efforts of "disruptive" apps, in particular, to circumvent existing government regulations. These characteristics, among others, pose new legal challenges for private parties, regulators, Attorneys General, and the courts.

The Federal Trade Commission (FTC) has the broadest reach in regulating mobile apps and does so most often through Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce."[38] Through this mechanism, the FTC has brought many enforcement actions for deceptive trade practices against companies for violation of their own privacy policies. FTC publications relating to mobile apps[39] emphasize the FTC's main privacy concern: companies must fulfill the promises they make, so as not to mislead consumers and they must get the consent of parents for interactions with children who are 13 and under. The FTC oversees and can bring enforcement actions related to the FTC Truth in Advertising Act,[40] the Fair Credit Reporting Act,[41] the Graham Leach-Bliley Act, [42] and the Children's Online Privacy Protection Act of 1998.[43] Other federal agencies, such as the Federal Communications Commission (FCC), the Office of Civil Rights (OCR) of the Department of Health and Human Services, the Food and Drug Administration (FDA), the Board of Governors of the Federal Reserve System, and the Securities and Exchange Commission (SEC) have an interest in and the power to regulate apps as they relate to telecommunication, protected health information under HIPAA,[44] medical devices and pharmaceutical products, mobile banking, and publicly traded securities, respectively.

---

38 15 U.S.C. § 45 (2006). *See also* FTC Policy Statement on Deception (Oct. 14, 1983), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception; *Cases and Proceedings*, FTC.GOV, https://www.ftc.gov/enforcement/cases-proceedings (last visited August 12, 2015).

39 *See Mobile Privacy Disclosures: Building Trust Through Transparency,* FTC STAFF REPORT (February 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. *See also Marketing Your Mobile App: Getting it Right from the Start* FTC (Sept. 2012), https://www.ftc.gov/system/files/documents/plain-language/pdf-0140_marketing-your-mobile-app.pdf. *See also Complying with COPPA: Frequently Asked Questions*, FTC (March 20, 2015), http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions.

40 15 U.S.C. §§ 41-58 requires all advertisements to be "truthful, not misleading, and, when appropriate, backed by scientific evidence. The Federal Trade Commission enforces these truth-in-advertising laws. When the FTC finds a case of fraud perpetrated on consumers, the agency files actions in federal district court for immediate and permanent orders to stop scams; prevent fraudsters from perpetrating scams in the future; freeze their assets; and get compensation for victims." *See also Truth in Advertising,* FTC, https://www.ftc.gov/news-events/media-resources/truth-advertising (last visited August 3, 2015).

41 15 U.S.C. § 1681. The FTC brings enforcement actions against credit reporting agencies, data brokers, and companies furnishing information to credit agencies to promote the "accuracy, fairness, and privacy of information in the files of consumer reporting agencies." *See also Credit Reporting,* FTC, https://www.ftc.gov/news-events/media-resources/consumer-finance/credit-reporting (last visited August 3, 2015).

42 15 U.S.C. § 6801 (2011), *et seq.* requires financial institutions to explain information sharing practices to consumers and safeguard personal and sensitive data.

43 5 U.S.C. §§ 6501-6505 (2010). Companies that fail to obtain express parental consent before collecting personal information online from children under age 13 are subject to FTC enforcement actions.

44 45 CFR §§ 160, 162, and 164 (1996).

While there is no comprehensive federal law regulating apps (a proposed "APPS Act"[45] failed to leave the House in 2013), this hasn't stopped state Attorneys General and state legislatures from taking their own action. California, in particular, has led the way by passing the California Online Privacy Protection Act (CalOPPA)[46] and amending it to address consumer tracking practices,[47] in addition to its pre-existing requirements that all websites and apps post conspicuous and accurate privacy policies.[48] The California Attorney General has sent a clear message to app developers and distributors, most recently, by promulgating extensive recommendations for mobile app privacy practices in the 2013, "Privacy on the Go: Recommendations for the Mobile Ecosystem" publication,[49] and by initiating the first-of-its-kind lawsuit against Delta Air Lines for failure to post an app privacy policy.[50] Prior to this, Attorney General Harris reached a 2012 agreement with Amazon, Apple, Google, Facebook, Hewlett-Packard, and others, to require the display of app privacy policies and subsequently sent warning letters to 100 mobile app companies giving them 30 days to post a conspicuous privacy policy.[51] The New Jersey Attorney General has also been active in regulating the app landscape, reaching settlements with two California-based app developers for alleged children's privacy violations,[52] and with an Ohio-based developer for allowing malware to "mine" app users' devices for virtual currencies.[53]

B. Where is Jurisdiction Proper?

As consumer app cases begin to enter courtrooms, the first line of defense to these cases is often a challenge to personal jurisdiction.[54] To recap, specific jurisdiction requires that a non-resident defendant (1) "purposefully directed" activities to the forum or one of its residents, or performed "some act by which he purposefully avails himself of the privilege of conducting

---

45 Application Privacy, Protection and Security Act of 2013, H.R. 1913, 113th Cong. (2013), *available at* https://www.govtrack.us/congress/bills/113/hr1913/text.

46 California Online Privacy Protection Act, Cal. Bus. & Prof. Code §§ 22575-22579 (2004), *available at* http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579.

47 California's AB 370 is an amendment to CalOPPA that requires entities that collect PII to disclose in a privacy policy how the entity treats "do not track" options enabled in web browsers, codified at: Cal. Bus. & Prof. Code § 22575(b)(5-6), *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB370.

48 CalOPPA, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).

49 Kamala D. Harris, *Privacy On The Go, Recommendations For The Mobile Ecosystem,* California Department of Justice (January 2013), *available at* http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

50 *People v. Delta Air Lines Inc.*, No. CGC 12-526741, 2013 WL 1951360 (Cal. Super. Ct. May 9, 2013) (dismissing complaint).

51 *Attorney General Kamala D. Harris Notifies Mobile App Developers of Non-Compliance with California Privacy Law,* State of California Department of Justice Office of the Attorney General (October 30, 2012), *available at* https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-notifies-mobile-app-developers-non-compliance.

52 Consent Decree and Order for Injunction and Other Relief, *Chiesa v. 24 x 7 Digital, LLC*, No. 2:12-cv-03402 (D.N.J. Jun. 26, 2012) (ECF No. 5).

53 *See New Jersey Division of Consumer Affairs, FTC, Reach Settlement with Developer of Mobile App that Allegedly Hacked New Jersey Smartphones with Harmful Malware,* State of New Jersey Office of the Attorney General (June 29, 2015), *available at* http://nj.gov/oag/newsreleases15/pr20150629a.html.

54 *See, e.g., Tomelleri v. Medl Mobile, Inc.*, No. 2:14-CV-02113-JAR, 2015 U.S. Dist. LEXIS 55943 at *8-40 (D. Kan. April 20, 2015) (granting dismissal for lack of personal jurisdiction and declining to transfer).

activities in the forum, thereby invoking the benefits and protections of its laws"; (2) the claim must "arise out of" defendant's forum related activities; and (3) the exercise of jurisdiction must comport with fair play and substantial justice, that is, it must be reasonable.[55]

General jurisdiction can be an even heavier lift for plaintiffs because with respect to an individual, the "paradigm jurisdiction" is the individual's domicile.[56] With respect to a corporation, *Bauman v. Daimler*[57] teaches that general jurisdiction only exists in the state where it is incorporated, where its principal place of business is located, or the state where its contacts are so continuous and systematic as to render it essentially "at home" in the state. Courts have been reluctant to rely on the "at home" exception and it is rarely evoked.[58]

The presence of Apple in Northern California resulted in a finding of specific jurisdiction in the Northern District of California for a consumer related case. In *Opperman v. Path, Inc.,*[59] plaintiffs sued seventeen defendants in the Western District of Texas in 2012, alleging that apps developed and distributed by defendants secretly uploaded and disseminated user information from the devices on which they were installed.[60] The Western District of Texas transferred the case to the Northern District of California, finding that "[a]ll allegations in this matter run through Apple and its app store."[61] The Northern District of California treated this ruling as law of the case and refused one defendant's invitation to revisit it.[62] If this theory of specific personal jurisdiction takes root in consumer cases, then the Northern District of California will be the hub for consumer-related app litigation.[63] General jurisdiction will also often be found in California because so many of the companies involved in creating and distributing apps are incorporated or headquartered in the state.

---

55 *See Schwarzenegger v. Fred Martin Motor Co.*, 374 F.3d 797, 802 (9th Cir. 2004).

56 *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S.—, 131 S.Ct. 2846, 2854 (2011).

57 571 U.S.—, 134 S.Ct. 746, 760-62 and n.9 (2014).

58 Discussing rigor of "essentially at home" test, *see Tomelleri v. Medl Mobile, Inc.*, No. 2:14-CV-02113-JAR, 2015 U.S. Dist. LEXIS 55943, at 8-12 (D. Kan. Apr. 29, 2015).

59 No. 13-cv-00453-JST, 2014 WL 246972 (N.D. Cal. Jan. 22, 2014).

60 *Id.*

61 Quoting the transfer order, *see id.* at 13.

62 *Id.* at 13-17.

63 Outside of the consumer context, courts do not necessarily adopt this theory of specific jurisdiction. For example, in a copyright infringement case relating to the Move the Box app, even though Move the Box app was sold through the Apple iTunes Store, the court ruled that defendants had not directed conduct causing injury to plaintiff, a non-California resident, in California. *See Zherebko v. Reutskyy,* No. C 13-00843 JSW, 2013 U.S. Dist. LEXIS 113493, 4-15 (N.D. Cal. Aug. 12, 2013). Nor does the mere sale of a company's products in a state confer jurisdiction there if someone other than the buyer alleges the claim. *In Intercarrier Communs. LLC v. WhatsApp Inc.*, No. 3:12-cv-776-JAG, 2013 U.S. Dist. LEXIS 131318 (E.D. Va. Sept. 13, 2013), the court found no jurisdiction over WhatsApp Inc. in the Eastern District of Virginia, when WhatsApp was a Delaware Corporation with its principal place of business in California. The court noted that WhatsApp's products were sold through third party stores (*e.g.* Apple's iTunes Store) and the third party—Apple—both collected payment and distributed the app to the purchaser. Under these circumstances, the fact that the app was available in Virginia, users used it there and WhatsApp collected data from users using in Virginia was not enough to establish personal jurisdiction over WhatsApp. *Id.* at 9-19.

C. Protecting Consumer Expectations.

Consumers bring individual and class action lawsuits, while regulators bring enforcement actions, both on their own volition and in conjunction with existing private suits, aimed at closing the gaps between the law and technology. The FTC has a keen interest in business practices that result in a gulf between what consumers expect and what is actually happening. In particular, app owners and distributors alike are facing major class action lawsuits related to children's in-app purchases (IAPs), as well as attempts by litigants to bring suits for the loss of IAPs and misleading advertising.

1. Minors' In-App Purchases.

Instances of children making hundreds and even thousands of dollars of in-app purchases on their parents' mobile devices have been garnering big headlines and lawsuits for the last several years.[64] App distributors have faced class action suits as well as FTC enforcements, while Amazon came under FTC scrutiny related to kids' in-app game purchases[65] and Facebook will face a class action suit in October 2015.[66] The app distribution platforms, rather than the apps in which purchases were made, were the subject of these suits and enforcements because, as a condition of making in-app sales, purchases had to go through the relevant app stores, which then retain a portion of the sale—usually 30%.

Class actions involving Apple[67] and Google[68] presented essentially the same facts and legal claims based on two novel arguments. First, parents argued that in-app purchases by a minor create a contract between the minor and the app store which parents may then disaffirm, while the app store argued that a minor's purchase is governed by the app stores' terms and conditions that the parent who owned the device agreed to by registering an account with the app store. The parents also argued that by marketing apps as "free" and failing to inform users that entering a password opened a 15 or 30 minute purchase window, the app store engaged in unfair or deceptive business in violation of the California Consumer Legal Remedies Act (CLRA)[69] and the California Unfair Competition Law (UCL).[70] Jurisdiction for both cases was in the Northern District of California, but the presiding Judges, Judge Davila in Apple and Judge Whyte in Google, came to different conclusions when deciding the motions to dismiss.

---

64 *See e.g.*, Chris Foresman, *Apple facing class-action lawsuit over kids' in-app purchases,* ARSTECHNICA.COM (April 15, 2011, 12:31 PM PDT), http://arstechnica.com/apple/2011/04/apple-facing-class-action-lawsuit-over-kids-in-app-purchases/. *See also Google facing US lawsuit over $66 of in-app purchases,* THE GUARDIAN, http://www.theguardian.com/technology/2014/mar/11/google-us-lawsuit-in-app-purchases (last viewed August 3, 2015).

65 Jeff John Roberts, *Amazon will battle the FTC over kids' in-app purchases, rejecting a Google-style settlement,* GIGAOM (October. 6, 2014, 4:02 PM PDT), https://gigaom.com/2014/10/06/amazon-will-battle-the-ftc-over-kids-in-app-purchases-rejecting-a-google-style-settlement/.

66 *See Bohannon v. Facebook*, No. 12-cv-01894-BLF, 2014 U.S. Dist. LEXIS 156281 (N.D. Cal. Nov. 3, 2014). Class certification granted in March 2015.

67 *In re Apple In-App Purchase Litig.*, 855 F. Supp. 2d 1030 (N.D. Cal. 2012).

68 *See Imber-Gluck v. Google, Inc.*, No. 5:14-01070-RMW, 2014 U.S. Dist. LEXIS 98899 (N.D. Cal. July 21, 2014).

69 Cal. Civ. Code § 1780, *et seq.*

70 Cal. Bus. & Prof. Code § 17200, *et seq.*

Judge Whyte granted Google's motion to dismiss on the contract and unfair competition issues, finding that the terms and conditions were unambiguous that the device owner would be responsible for all purchases made in the app store, and that the plaintiffs failed to allege that they were unaware of a 30-minute password window.[71] However, Judge Whyte denied Google's motion to dismiss the UCL claim for misleading advertising based on the allegation that Google's practice of marketing apps as free was likely to deceive the public.[72]

On the other hand, Judge Davila denied Apple's motion to dismiss on all of these issues, finding, with respect to the contract issue, that Apple had failed to cite any case law supporting the contention that terms and conditions for the app store govern all subsequent purchases.[73] With respect to the unfair competition claims, Judge Davila found one plaintiff's assertion that she downloaded an app for her son because it was free, and more than one plaintiffs' assertion that they were not informed by Apple of the 15-minute password window to be sufficient to move forward with the UCL and CLRA claims.[74] Ultimately, the cases did not proceed very far.

Apple[75] and Google[76] also faced FTC enforcement actions for deceptive practices concurrently with these lawsuits. Apple settled with the class litigants in February 2013 to allow over 23 million in-app purchasers to receive a $5 credit, and subsequently, settled with the FTC for $32.5 million. As a condition of settlement, the FTC specifically required Apple to implement measures designed to obtain informed, express consent prior to every in-app charge, and, if Apple obtains consent for future charges, such as a periodic replenishment, it must give consumers the option to withdraw consent at any time.[77] Now Apple requires password entry immediately before every purchase and has eliminated the 15-minute password window. Google settled with the FTC for $19 million in September 2014[78] and avoided class certification in March 2015 because most class members would have been covered in the FTC settlement.[79]

Writing in dissent to the Apple settlement, FTC Commissioner Joshua D. Wright argued that the penalty was out of proportion to the "miniscule" percentage of Apple customers who were allegedly injured and could hamper innovation.[80] On the other hand,

---

71 *Imber-Gluck*, 2014 U.S. Dist. LEXIS 98899 at 11-12, 17.

72 *Id.*

73 *In re Apple In-App Purchase Litig.*, 855 F. Supp. 2d at 1030, 1036.

74 *Id.*

75 Complaint, *In the Matter of Apple Inc., A Corp.*, 112-3108, *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115applecmpt.pdf.

76 Complaint, *In the Matter of Google Inc., A Corp.*, 122-3237, *available at* https://www.ftc.gov/system/files/documents/cases/140904googleplaycmpt.pdf.

77 Agreement Containing Consent Order, *In the Matter of Apple Inc., A California Corp.*, 112-3108 (Jan. 15, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115appleagree.pdf.

78 Agreement Containing Consent Order, *In the Matter of Google Inc., A Corp.*, 122-3237 (Sept. 4, 2014), https://www.ftc.gov/system/files/documents/cases/140904googleplayorder.pdf.

79 Order Granting Motion to Deny Class Certification, *Imber-Gluck v. Google, Inc.*, No. 5:14-cv-01070-RMW (N.D. Cal. Apr. 3, 2015), *available at* http://classifiedclassaction.com/wp-content/uploads/2015/04/imber-gluck-v-google.pdf.

80 Agreement Containing Consent Order, *In the Matter of Apple Inc., A California Corp.* (Jan. 15, 2014), *available at* https://www.ftc.gov/sites/default/files/documents/cases/140115appleagree.pdf.

consumer advocates note that even the new password entry system is flawed in that it only exists within certain iOS operating systems.[81] Others continue to press for better labeling of freemium apps.[82]

An FTC enforcement action against Amazon is underway as of the time of this publication in the Western District of Washington.[83] The FTC is seeking an injunction requiring refunds to consumers for unfairly billing Amazon account holders for charges made by children without the account holder's consent.[84] At the introduction of IAPs, Amazon required no password entry; it later implemented a password requirement with a fifteen-minute window for any IAP of $20 or more.[85] However, shortly before the FTC filed its complaint, Amazon updated its billing practices to obtain the account holder's informed consent prior to every purchase on its newer mobile devices. As a result, Amazon has indicated that it intends to fight the enforcement action and will not settle with the FTC.[86]

2. Misleading Advertising.

Misleading advertising claims related to the functionality of specific apps have not found a successful path yet. Class action suits were filed against Apple for misleading advertising related to its Apple Maps for iPhone 5,[87] which failed to perform as depicted in advertisements, and related to Siri,[88] which occasionally malfunctioned. In both cases the court found that the plaintiffs failed to allege the specific fraudulent statement made by Apple, reasoning that plaintiffs did not allege that Apple said the apps would never malfunction.[89]

3. Virtual Currency.

Apps that deploy their own virtual currency are exposed to an additional array of potential legal issues. For example, if the user expends some currency to play the game again or to play a higher level, but the game malfunctions for some reason, that could impose liability absent a refund of the virtual currency or equivalent credit. Games with virtual currency can also give rise to securities claims. In at least one case, a company involved in online gaming was sued for securities fraud for failing to disclose the portion

---

81 Rene Ritchie, *In-app purchases and the App Store: What every parent needs to know*, IMORE.COM (July 18, 2014, 7:36 pm EDT), http://www.imore.com/app-purchases-and-app-store-what-every-parent-needs-know.

82 *Id.*

83 *F.T.C. v. Amazon.com, Inc.*, No. C14-1038, 71 F. Supp. 3d 1158 (W.D. Wash. Dec. 1, 2014).

84 Complaint for Permanent Injunction and Other Equitable Relief, *F.T.C. v. Amazon.com, Inc.,* No. C14-1038 (W.D. Wash. Jul. 10, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/140710amazoncmpt1.pdf.

85 *FTC Alleges Amazon Unlawfully Billed Parents for Millions of Dollars in Children's Unauthorized In-App Charges,* FTC (July 10, 2014), https://www.ftc.gov/news-events/press-releases/2014/07/ftc-alleges-amazon-unlawfully-billed-parents-millions-dollars.

86 *Amazon says it will fight FTC on in-app purchases made by children,* LA TIMES (July 2, 2014), http://www.latimes.com/business/technology/la-fi-tn-amazon-ftc-kids-20140702-story.html.

87 *Minkler v. Apple, Inc.*, 65 F. Supp. 3d 810, 820-21 (N.D. Cal. 2014).

88 *In re iPhone 4S Consumer Litig.*, No. C 12-1127 CW, 2014 U.S. Dist. LEXIS 19363, at *4-9 (N.D. Cal. Feb. 14, 2014).

89 *Minkler,* 65 F. Supp., at 816-21 (dismissing with leave to amend); *iPhone 4S Consumer Litig.*, 2014 U.S. Dist. LEXIS 19363, at *14-30 (dismissing without leave to amend).

of its disclosed users who were "gold farmers"—that is people who play a game to exploit in-app opportunities to acquire virtual currency and then sell it in the real world—and that the number of users would be negatively affected by an undisclosed rule change that curtailed gold farming.[90] Another issue with gold farming is that it can create inflation in a game, detracting from the value for other players.[91] Risk also arises if the app owner pairs with partners to offer promotional ways to acquire virtual currency, without full disclosure of how the partner will interact with consumers who take advantage of the promotion.[92] A decision to discontinue a game or to alter or discontinue its virtual currency in which consumers have invested can also give rise to claims.[93]

D. Preserving and Redefining Consumer Privacy.

While apps may provide at least a basic privacy policy,[94] few mobile users seem to be aware of the depth and breadth of data their apps collect and share. Over three-quarters of Americans consider data stored on their mobile device to be as private as information stored on their home computer, and 81% percent of those surveyed by the Berkeley Center for Law and Technology would not want a social media site to access their contacts to suggest connections.[95] Furthermore, over half of app users surveyed by the Pew Research Center in 2012 decided not to install an app after they were informed of how much data the app would collect, and 30% decided to uninstall the app after learning the same.[96] The fervor at which app owners are interested in collecting user data is clearly not reflected in mobile users' expectations, or even understandings, of the apps they use.

Private parties and regulators are undertaking efforts to preserve and redefine privacy in an ever-changing technological landscape by imposing either formal requirements or informal guidelines that apps that collect personally identifiable information (PII) have privacy policies. The National Institute of Standards and Technology defines PII as: "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as a name, social

---

90 *See In re Giant Interactive Group, Inc. Sec. Litig.*, 643 F. Supp. 562, 569 -74 (S.D.N.Y. 2009). This complaint survived a motion to dismiss.

91 *Id.* at 567-68.

92 *Cf. Swift v. Zynga Game Network, Inc., No.* C 09-05443 SBA, 2010 U.S. Dist. LEXIS 117355, at *2-8 (N.D. Cal. Nov. 3, 2010) (consumer in putative class action alleged that when they participated in promotional offers to obtain virtual currency, they ended up obtaining goods or services they did not want or need and that obtaining cancellation or refund was thwarted).

93 *Cf. Abreau v. Slide*, No. C 12-00412 WHA, 2012 U.S. Dist. LEXIS 47217, at *2-5 (N.D. Cal. Apr. 3, 2012) (consumer brought putative class actions when online game was cancelled because the game's virtual currency, "gold," would then not have value).

94 Note, however, that many apps do not provide even a basic privacy policy, or do not provide adequate information: a recent Future of Privacy Forum survey "found that 22 out of the 30 most popular mobile apps lacked even a basic privacy policy where consumers could learn about what data is collected or exchanged when they download the app." *See Future of Privacy Forum Launches App Privacy Site,* Future of Privacy Forum, http://www.futureofprivacy.org/2011/05/26/future-of-privacy-forum-launches-app-privacy-site/ (last visited August 3, 2015).

95 Jennifer M. Urban, Chris Jay Hoofnagle, & Su Li, *Mobile Phones and Privacy,* U.C. Berkeley Public Law Research paper No. 2103405 (July 10, 2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

96 Jan Lauren Boyles, Aaron Smith, & Mary Madden, *Privacy and Data Management on Mobile Devices,* Pew Internet & Am. Life Project (Sept. 5, 2012), *available at* http://pweinternet.org/Reports/2012/Mobile-Privacy.aspx.

security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[97] So, for instance, data that might not otherwise be classified as PII, such as geolocation or IP address, would be classified as PII if it can be linked to an individual.

Privacy policy requirements are enforceable under Section 5 of the FTC Act, as well as state laws such as CalOPPA,[98] and statutes in Connecticut,[99] Pennsylvania,[100] and Nebraska.[101] CalOPPA is the most extensive of these laws in that it affirmatively requires websites that collect information from consumers in California to conspicuously post a privacy policy and fulfill other specific requirements.[102] To comply with California law, the California Attorney General guidelines, the FTC's expectations, and more, mobile app privacy policies, generally, should disclose: (1) what information is collected from users when they use an app, no matter whether the data is PII or not; (2) how the information is used (for example, for analytics purposes) even if the users do not have to enter any PII to use the app; (3) how the information is disclosed or shared with third parties; (4) how users can update or remove personal information and notice as to how users will be informed in the event that the privacy policy changes. Most problems arise in connection with the third requirement. While most concerns center around the disclosure of PII for profit-seeking purposes, even the disclosure of anonymized and aggregated data for analytics purposes without user consent can result in litigation.[103]

Consumers have brought significant lawsuits against companies for failure to properly disclose information collection and sharing practices in their app privacy policies. In *Opperman v. Path,* plaintiffs alleged that sixteen app developer defendants secretly uploaded and disseminated user information from devices on which the apps were installed, and that a final defendant, Apple, was complicit in allowing the apps, available in the App Store and downloaded to Apple devices, to do so.[104] Plaintiffs brought a variety of claims under California and federal laws[105] all but one of which were dismissed for failure to demonstrate that plaintiffs relied upon the allegedly deceptive privacy policies in purchasing Apple

---

97 Erika McCallister, Tim Grance, & Karen Scarfone, *Guide to protect the confidentiality of personally identifiable information,* NIST (April 2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

98 Cal. Bus. & Prof. Code § 22575-22579 (2004).

99 Conn. Gen. Stat. § 42-471 (2009).

100 18 Pa. C.S.A. § 4107(a)(10) (2005) (prohibiting misleading statements on websites under state Fraudulent Business Practices Statute).

101 R.R.S. Neb. § 87-302 (14) (2003) (prohibiting making knowingly false statements in privacy policy).

102 CalOPPA, Cal Bus. & Prof. Code §§ 22575-22579 (2004). The privacy policy must identify the categories of PII that the Company collects, the categories of third parties with which the Company may share the information, the process by which consumers may review and request changes to their PII, and the process the company will undertake in notifying customers of changes to the privacy policy.

103 *See* California Bookkeeping Statute, Cal. Civ. Code §1799, *et seq.* (prohibiting disclosure of aggregate financial data to third parties without data owner's consent in traditional bookkeeping context).

104 *Opperman v. Path*, No. 13-CV-00453-JST, 2014 WL 1973378 (N.D. Cal. May 14, 2014) (order denying in part and granting in part defendants' motions to dismiss).

105 Claims included violation of the California UCL, the False and Misleading Advertising Law, the CLRA, the Comprehensive Computer Data Access and Fraud Act, and the California Wiretap Act, as well as the federal Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, among others.

devices.[106] Although the defendants dodged potentially huge liability, the lawsuit led to a public apology by the Path app, Apple's revision of its privacy settings, and the initiation of a Senate investigation into public allegations that Apple encourages apps to surreptitiously collect information from mobile devices in violation of its outward-facing policy.[107]

Plaintiff, Svenson, on the other hand successfully survived motions to dismiss related to breach of contract and UCL claims against dissemination of user information to app developers upon a user's purchase of that app.[108] Judge Labson Freeman, relying on the Ninth Circuit's 2014 *In re Facebook Privacy Litigation*[109] decision, which held that Facebook users were "harmed both by dissemination of their personal information and by losing the sales value of that information," found that the mobile app user plaintiff had stated a claim for breach of contract based on the diminution of value of her information as well as a loss of the benefit of the bargain.[110] The plaintiff's UCL claim also survived.[111] As of the publication of this article, this case was still pending in the Northern District of California.

The FTC is also active in bringing enforcement actions related to misleading privacy policies in apps. Most notably, the FTC obtained a settlement[112] against Snapchat—an app that's main selling point was its privacy—for misleading consumers that photos and videos taken through the app "disappear forever" when they did not.[113] Snapchat had also failed to inform users of its collection and use of geolocation data, as did Goldenshores in its Flashlight App.[114] The FTC was particularly concerned with the Flashlight App collection of geolocation data because such a practice would not have been expected by consumers, nor necessary for the app to function.[115] The FTC has further emphasized the need for transparent and accurate disclosures related to the collection of geolocation data through its Congressional testimony in 2014[116] and a 2015 publication on the topic.[117]

---

106 *See Opperman*, 2014 WL 1973378.

107 *See* Sarah Gilbert, *Apple, App Makers Escape iDevice Snooping Class Action Lawsuit,* TOPCLASSACTIONS.COM (May 19, 2014), http://topclassactions.com/lawsuit-settlements/lawsuit-news/27439-apple-app-makers-escape-idevice-snooping-class-action-lawsuit/. See also, *Espitia v. Hipster, Inc.*, No. 3:13-cv-00432, (N.D. Cal. Aug. 13, 2013) (alleging similar facts and claims and resulting in public apology by Hipster app), *available at* http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1419&context=historical.

108 *Svenson v. Google Inc.*, No. 13-CV-04080-BLF, 2015 WL 1503429 (N.D. Cal. 2015).

109 *Facebook Privacy Litig. v. Facebook, Inc.,* 572 Fed. Appx. 494 (9th Cir. 2014).

110 *Svenson*, 2015 WL 1503429 at 5.

111 *Id.* at 10.

112 Decision and Order, *In the Matter of Snapchat, Inc., A Corp.*, 132-3078 (Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.

113 *See FTC Approves Final Order Settling Charges Against Snapchat,* FTC (December 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat.

114 Agreement Containing Consent Order*, In the Matter of Goldenshores Technologies, Inc. and Erik M. Geidl*, 132-3087 (Dec. 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/131205goldenshoresorder.pdf.

115 *Id.*

116 *FTC Testifies on Geolocation Privacy,* FTC (June 4, 2014), https://www.ftc.gov/news-events/press-releases/2014/06/ftc-testifies-geolocation-privacy.

117 *Location, location, location, FTC* (February 11, 2015, 9:59 AM), https://www.ftc.gov/news-events/blogs/business-blog/2015/02/location-location-location.

Highly-regulated categories, such as children, health, and finance are associated with even stricter privacy policy requirements. If children will be using an app or will be inherently drawn to an app, there are particularly onerous privacy policy requirements under COPPA, on which the FTC has issued guidelines[118] and conducted a study.[119] Mobile apps must not collect PII from users under age 13 and if an app does collect PII, the app's owner should take several measures to avoid any liability under COPPA. The measures include: explicitly stating in the app privacy policy that the app is not intended for use by anyone under age 13; requiring users to certify that they are over age 13 and enter their birthday; or requiring users to connect to the app via Facebook Connect, as Facebook requires its users be at least 13 years old. In 2011, in its first enforcement action against a mobile app, the FTC handed the BrokenThumbs children's game app a $50,000 penalty for collecting and disseminating children's' information without parental consent.[120]

E. Imposing Data Protection Requirements.

A number of states have passed legislation requiring companies to protect PII by imposing specific security measures, refraining from sharing or selling consumers' PII, and ensuring secure disposal of PII.[121] The depth and detail of these laws varies by state, but an app owner may be held accountable if it does not reasonably secure user information. Additionally, the FTC has brought claims under Section 5 of the FTC Act charging companies with engaging in unfair practices by implementing "unreasonable" security practices.[122] Although both Apple and Google provide default data security protections in their mobile operating systems, which are then automatically incorporated into apps running on those platforms, some apps have found a way to disable the security features. This was the case with the Credit Karma and Fandango apps, which purposefully overrode the standard security processes, exposing customers' payment information to interceptions.[123] In March 2014, the FTC secured settlements against both of these companies for their failures to take reasonable steps to secure the transmission of consumers' personal data through their apps.[124]

Other federal agencies are also ruling on data protection requirements. For example, the FCC ruled that the FCC Act requiring protection of consumer information such as call logs, call duration and phone numbers extends to mobile devices and pre-installed mobile

---

118 *Complying with COPPA: Frequently Asked Questions, FTC* (March 20, 2015), http://www.business.ftc.gov/documents/0493-Complying-with-COPPA-Frequently-Asked-Questions.

119 *Mobile Apps for Kids,* FTC (February 2012), https://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf.

120 *United States v. W3 Innovations, LLC*, No. CV-11-03958, 2011 U.S. Dist. LEXIS 100914 (N.D. Cal. Sept. 8, 2011). Consent Decree and Order *available at* https://www.ftc.gov/sites/default/files/documents/cases/2011/09/110908w3order.pdf.

121 *See* Cal. Civ. Code §1798.81 (2010). *See also* Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.03 (2015).

122 Federal Trade Commission Act, Sec. 5, 15 U.S.C. § 45.

123 Complaint, *In the Matter of Fandango, LLC*,132-3089, *available at* https://www.ftc.gov/system/files/documents/cases/140328fandangocmpt.pdf; Complaint, *In the Matter of Credit Karma, Inc.*, 132-3091, *available at* https://www.ftc.gov/system/files/documents/cases/140328creditkarmacmpt.pdf.

124 Decision and Order, *In the Matter of Fandango, LLC*,132-3089, *available at* https://www.ftc.gov/system/files/documents/cases/140819fandangodo.pdf; Decision and Order, *In the Matter of Credit Karma, Inc.*, 132-3091, *available at* https://www.ftc.gov/system/files/documents/cases/1408creditkarmado.pdf.

apps. Protected information under the Act also includes geolocation data about where a call starts and ends.[125] However, apps that are not pre-installed on mobile devices are free to collect and use data without concern for the FCC Act, as are mobile providers that do not fall into the regulated category of telecommunications providers.[126]

Furthermore, forty-seven states, Guam, Puerto Rico, the Virgin Islands, and the District of Columbia have laws imposing notification requirements on entities in the event of unauthorized access to PII.[127] Failure to comply with such laws can be costly. State Attorneys General can and do bring enforcement actions and cooperate on multi-state data breach investigations, as they have in the high-profile breaches of Anthem, Target, and the Internal Revenue Service.

While many may be familiar with the headline-garnering security breaches at well-known corporations like Sony[128] and Neiman Marcus, among others, mobile apps are quickly becoming hackers' new targets because of the sheer volume and complexity of valuable data they collect, as well as the recent decline in PC use. However, Gartner, Inc. found that hackers don't need to be technically sophisticated to access mobile data: 75% of "[m]obile security breaches are—and will continue to be—the result of misconfiguration and misuse on an app level, rather than the outcome of deeply technical attacks on mobile devices."[129] Another entity has identified 1,500 iPhone apps that contain a "crippling bug" making iPhones extremely vulnerable to hackers' attempts to obtain passwords, bank account numbers, and other sensitive data.[130] Dating apps, in particular, pose serious security risks due to users' willingness to share personal information and respond to messages that may contain harmful malware, making BYOD company data vulnerable to breach.[131] These factors combined with a finding that 60% of popular dating apps for Android had medium or high security vulnerabilities and one in ten Americans have used a dating site or app, make dating apps an especially concerning category of apps.[132]

---

125 For the FCC's declaratory ruling see 28 FCC Rcd 9609, 9609, 2013 FCC LEXIS 2834, 58 Comm. Reg. (P & F) 739, 2013 FCC LEXIS 2834, 58 Comm. Reg. (P & F) 739 (F.C.C. 2013), *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2013/db0628/FCC-13-89A1.pdf.

126 *Id.*

127 Under Section 1798.82(a) of the California Civil Code, a business that is the target of a security breach must notify any California resident that his or her information was acquired, or reasonably believed to have been acquired, by an unauthorized person. The law further requires that a business report a security breach to the California Attorney General's Office if more than 500 California residents were subject to the breach.

128 Jeffrey Roman, *Sony Settles Data Breach Lawsuit Data Breach Today,* DATA BREACH TODAY (June 16, 2014), http://www.databreachtoday.asia/sony-settles-data-breach-lawsuit-a-6960#.

129 *Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration,* GARTNER (May 29, 2014), http://www.gartner.com/newsroom/id/2753017.

130 Dan Goodin, *1,500 iOS apps have HTTPS-crippling bug. Is one of them on your device?,* ARSTECHNICA.COM (April 20, 2015, 2:08 PM PDT), http://arstechnica.com/security/2015/04/1500-ios-apps-have-https-crippling-bug-is-one-of-them-on-your-device/.

131 Nicole Arce, *Using Dating Apps On Company Smartphone? You Might Be Putting Trade Secrets At Risk,* TECH TIMES (February 13, 10:20 PM), http://www.techtimes.com/articles/32399/20150213/using-dating-apps-on-company-smartphone-you-might-be-putting-trade-secrets-at-risk.htm.

132 *IBM Security Finds Over 60 Percent of Popular Dating Apps Vulnerable to Hackers,* IBM, https://www-03.ibm.com/press/us/en/pressrelease/46023.wss (last viewed August 3, 2015).

F. Developing Comprehensive App Terms of Use.

Terms of Use are a legal agreement between an app owner and every user of the app. An app user automatically agrees to the terms by downloading the app. The Terms of Use set forth what the app is, how it should be used, what constitutes improper use, and what the consequences of improper use will be. Terms of Use should be present in every app that requires interactivity or that collects any personal information.

Many apps present opportunities for misuse; comprehensive Terms of Use can help protect app owners from liability if a user violates federal or state laws. However, as the potential uses for apps become more complex and unexpected, there is an increasing gap between expectations of the public, the laws that cover certain behavior, and the capabilities of mobile apps. For example, live streaming video apps Meerkat and Periscope launched in spring 2015 and took the app world by storm.[133] Both apps allow users to stream live video footage directly onto social media without any opportunity to review or cut footage. Brand marketers have taken a quick liking to the apps because of the ability to capture real-world footage of people using advertised products. However, posting live video of individuals for profit without their consent could come with hefty risk.[134] This technology also poses serious potential for copyright infringement. Although the Twitter-owned Periscope warns users against streaming copyrighted material in its Terms of Use, HBO issued take-down notices to Periscope within months of its launch after users broadcast a Game of Thrones episode through the app.[135] It is important for apps entering new technological frontiers to evaluate and protect against potential risk, especially risk that could imperil the whole venture.

Similarly, apps that collect facial recognition data for commercial use such as the NameTag app[136] are unleashed in a regulatory and legal environment that has not accounted for them yet. To the extent they present serious privacy concerns and can be used for commercial gain by tracking consumer habits, they need to plan for change in the legal and regulatory landscape. As the proliferation of up-to-the-second live footage and facial recognition apps become more and more common, courts and regulators will surely attempt to make legal innovations to allow the law to catch up with technology.

G. Regulating Industries For Consumer Safety And Fair Competition.

Regulated industries such as common carrier transportation, housing, hotels, medical devices, health providers, insurance, and even aviation are facing innovative technological advances and business models, fueled, oftentimes, by the "sharing economy" that threaten to disrupt—or have already disrupted—their fundamental modes of operation. "Disruptive technology" businesses, such as Uber, Lyft, Airbnb, and Zenefits, to name a few, often operate mainly or even entirely through mobile apps and are associated with a widespread

---

133 Zach Miners, *Live streaming apps like Meerkat and Periscope pose legal risks for users,* PC WORLD (April 20, 2015, 1:27 PM), http://www.pcworld.com/article/2912272/live-streaming-apps-pose-legal-risks-for-users.html.

134 Live stream footage captured for commercial purpose without consent could present private cause of action. *See id*.

135 Natalie Jarvey, *HBO Criticizes Periscope Over 'Game of Thrones' Live Streams, Issues Takedown Notices,* HOLLYWOODREPORTER.COM (April 14, 2015, 1:32 PM PDT), http://www.hollywoodreporter.com/news/hbo-criticizes-periscope-game-thrones-788734.

136 For name tag app, *see* http://www.nametag.ws/.

belief that their innovative business models should fall outside the existing regulatory framework. However, the sharing economy has exploded—according to one study, there are now 17 billion-dollar companies with approximately 60,000 employees in the sharing economy—and regulators, not surprisingly, are taking notice.

Ride-sharing companies like Uber and Lyft have been the scapegoat of the taxi cab industry's woes,[137] but have also faced increasing scrutiny from district attorneys nationwide, seeking to subject the companies to pre-existing taxi regulations. The District Attorneys for Los Angeles and San Francisco are taking action against Uber and Lyft for using fare calculations that are not approved by the state,[138] while the California Labor Commission recently ruled that Uber must treat its drivers as employees rather than independent contractors.[139] The examples do not end with ride-sharing companies. Municipal regulations that prohibit short-term housing may stifle Airbnb in major U.S. cities, and apps like FlightCar, which facilitates rentals of private car owners' vehicles, and EatWith, which connects diners with home chefs, are battling car rental regulations and health code violations, respectively.[140]

Beyond the sharing economy, innovative and potentially life-saving health and medical apps, which generated an estimated $718 million worldwide in 2012 and grow in number by 150% a year, are coming under fire by the FDA and FTC.[141] The FTC hit MelApp and Mole Detective, two apps that purported to diagnose melanoma with the snap of a photo, with a deceptive practices claim based on a lack of scientific evidence to back up the apps' advertised diagnosis capabilities.[142] In February 2015, the FDA released guidelines[143] asserting jurisdiction over "mobile medical apps" that are intended for use in diagnosing medical conditions "and whose functionality could pose a risk to the patient's safety if the mobile app were not to function as intended."[144] Despite the recent publication, this has long been the FDA's practice: remote X-ray, MRI and CT imaging app Nephosity sought FDA

---

137 Rubin, Alissa and Scott, Mark, *Clashes Erupt Across France as Taxi Drivers Protest Uber,* New York Times (June 25, 2015), http://www.nytimes.com/2015/06/26/business/international/uber-protests-france.html?_r=0.

138 Ellen Huet, *SF, LA District Attorneys Sue Uber, Settle with Lyft Over 'Misleading' Business Violations,* Forbes.com (December 9, 2014), http://www.forbes.com/sites/ellenhuet/2014/12/09/sf-la-district-attorneys-sue-uber-and-lyft-over-misleading-business-violations/.

139 *Berwick v. Uber Technologies, Inc.*, No. 11-46739, California Labor Commission, *available at* http://www.scribd.com/doc/268911290/Uber-vs-Berwick.

140 Andrew Bender, *New Regulations To Wipe Out 80% Of Airbnb Rentals In California's Santa Monica,* Forbes.com (June 15, 2015, 3:55 PM), http://www.forbes.com/sites/andrewbender/2015/06/15/new-regulations-to-wipe-out-80-of-airbnb-rentals-in-californias-santa-monica/.

141 Dina ElBoghdady, *Health-care apps for smartphones pit FDA against tech industry,* The Washington Post (June 22, 2012), *available at* http://www.washingtonpost.com/business/economy/health-care-apps-for-smartphones-pit-fda-against-tech-industry/2012/06/22/gJQAHCcBvV_story.html.

142 *FTC Cracks Down on Marketers of 'Melanoma Detection' Apps,* FTC (February 23, 2015), https://www.ftc.gov/news-events/press-releases/2015/02/ftc-cracks-down-marketers-melanoma-detection-apps.

143 *Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff*, U.S. Department of Health and Human Services Food and Drug Administration, Center for Devices and Radiological Health & Center for Biologics Evaluation and Research (February 9, 2015), *available at* http://www.fda.gov/downloads/MedicalDevices/ . . . /UCM263366.pdf.

144 *Id.* at 4.

clearance in 2008, finally gaining approval in 2013[145] and Sanofi's glucose monitor app, the iHealth blood pressure monitor, and WiThing's body-fat percentage tracker all obtained FDA approval before hitting the market.[146]

What the recent guidelines do make clear, however, is that there is a broad range of mobile health apps that fall outside the definition of a "medical device" and therefore are not subject to FDA approval prior to market availability.[147] Such apps include activity trackers, diet logs, BMI calculators, medical reference apps, and apps that facilitate video communication between patients and providers (termed "telemedicine" and garnering serious HIPAA concerns), to name a few of the more than 18,000 health-related apps in existence as of 2012.[148] The amalgamation of such extensive health and medical data, especially if not within the purview of the FDA, in combination with the data already being collected is beginning to catch the eye of consumer advocates and regulators.

These examples demonstrate that regardless of apps' attempts to operate outside the existing regulatory framework, regulators will no longer ignore consumers' unprecedented level of app use, the revenue these apps generate, or their own duty to protect public interests in regulated industries. A failure by app developers and investors to heed existing regulations in advance of launching new businesses could easily expose the company to growth-crippling regulatory actions.

V. CONCLUSION.

Apps represent a burgeoning component of the California economy. With the meteoric rise in spending on apps during this decade, apps and the relationships they create with consumers are moving front and center in companies' asset portfolios and are garnering the attention of regulators and plaintiffs' attorneys alike. Plaintiffs' lawyers are currently testing various theories to find a footing that will lead to large damage awards. California courts will likely lead the way in resolving disputes relating to apps. Companies, whether they use apps as the centerpiece to drive their business or as a way of enhancing existing products and services, need to understand that the constellation of legal and regulatory considerations that factor into managing an apps portfolio is both complex and constantly evolving.

---

145 Neil Versel, *FDA clears Nephosity iPad app for diagnostic imaging,* Mobi Health News (May 22, 2013) http://mobihealthnews.com/22554/fda-clears-nephosity-ipad-app-for-diagnostic-imaging/.

146 ElBoghdady, *supra* note 141.

147 *Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff, supra* note 143.

148 *Id.*