Journal of Business & Technology Law

Volume 14 | Issue 1 Article 4

Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures

Ronan Ó. Fathaigh

Joris van Hoboken

Nico van Eijk

Mobile Privacy and Business-to-Platform Dependencies: An Analysis of SEC Disclosures

RONAN Ó FATHAIGH, JORIS VAN HOBOKEN & NICO VAN EIJK*

This Article systematically examines the dependence of mobile apps on mobile platforms for the collection and use of personal information through an analysis of Securities and Exchange Commission (SEC) filings of mobile app companies. The Article uses these disclosures to find systematic evidence of how app business models are shaped by the governance of user data by mobile platforms, in order to reflect on the role of platforms in privacy regulation more generally. The analysis of SEC filings documented in the Article produces new and unique insights into the data practices and data-related aspects of the business models of popular mobile apps and shows the value of SEC filings for privacy law and policy research more generally. The discussion of SEC filings and

* Ronan Ó Fathaigh, Researcher, Institute for Information Law, University of Amsterdam; Prof. Dr. Joris van Hoboken, Senior Researcher, Institute for Information Law, University of Amsterdam and Professor of Law, Vrije Universiteit Brussels; and Prof. Dr. Nico van Eijk, Professor of Information Law, and Director, Institute for Information Law, University of Amsterdam, the Netherlands. The authors would like to thank the participants of the 2018 Privacy Law Scholars Conference at the George Washington University School of Law for very helpful comments on an earlier draft. This paper is part of a multidisciplinary research project of the University of Amsterdam and MIT on transparency in smartphone ecosystems, funded by the Dutch National Science Foundation (NWO) and NSF. The project addresses the question of how transparency requirements in data privacy law map to the smartphone context, looking at the way in which different regulatory environments for data privacy (E.U. and U.S.) shape transparency about the collection and use of personal data in dominant smartphone ecosystems (Android and Apple iOS).

privacy builds on regulatory developments in SEC disclosures and cybersecurity of the last decade. The Article also connects to recent regulatory developments in the U.S. and Europe, including the General Data Protection Regulation, the proposals for a new ePrivacy Regulation and a Regulation of fairness in business-to-platform relations.

CONTENTS

INTRODUCTION

Activision Blizzard Inc., which acquired the developer of the *Candy Crush Saga* mobile application for $5.8 billion in 2016, sounded a warning note in its February 2018 filings with the U.S. Securities and Exchange Commission ("SEC") about its dependence on mobile platforms. Activision explained that if these platforms, such as Apple's App Store or the Google Play store, "change how the personal information of consumers is made available to developers, [its] business could be negatively impacted."[1] Similarly, Facebook Inc., with revenues of $40.6 billion in 2017, also warned in its SEC

[1] Activision Blizzard, Inc., Annual Report (Form 10-K) 21 (Feb. 27, 2018).

filings about its dependence on mobile platforms. Given that nearly 90 percent of its revenue is now generated from advertising on mobile devices, any changes by mobile platforms which "limit [its] ability to deliver, target, or measure" advertising on mobile devices could "adversely affect . . . monetization on mobile devices."[2]

This Article examines the dependence of mobile apps on mobile platforms for the collection, use and monetization of personal information. In particular, the Article explores how app business models are shaped by the governance of user data by mobile platforms, and what the implications may be for the position of mobile platforms in privacy regulation.[3] Most privacy regulations in the U.S. and Europe do not provide for specific obligations of mobile platforms, except for a number of issued recommendations and a provision on privacy settings in Article 10 of the recently proposed ePrivacy Regulation in the E.U.[4] In the broader context of online platforms, the European Commission has begun to examine business-to-platform relationships, which is an "under-researched subject, both empirically and theoretically."[5] This Article seeks to contribute to the

[2] Facebook, Inc., Annual Report (Form 10-K) 10 (Feb. 1, 2018).

[3] *See* Daniel Greene & Katie Shilton, *Platform Privacies: Governance, Collaboration, and the Different Meanings of "Privacy" in iOS and Android Development*, 20 NEW MEDIA & SOC'Y 1640 (2018), available at https://doi.org/10.1177/1461444817702397 (discussing the meaning of privacy on the iOS and Android platforms); *see also* Katie Shilton & Daniel Greene, *Linking Platforms, Practices, and Developer Ethics: Levers for Privacy Discourse in Mobile Application Development*, J. BUS. ETHICS (Mar. 28, 2017), available at https://doi.org/10.1007/s10551-017-3504-8 (discussing when and how privacy conversations arise during mobile application development).

[4] *Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC*, COM (2017) 10 final (Jan. 10, 2017).

[5] EUROPEAN COMMISSION, BUSINESS-TO-BUSINESS RELATIONS IN THE

understanding of such business-to-platform dependencies in the mobile app environment, particularly relating to the use of personal information.

To understand this dependence, this Article examines the SEC filings of U.S. public companies that predominantly operate their business, or important parts of their business, as popular apps in the mobile app ecosystem. Our approach is motivated by a series of initial public offerings (IPOs) by major mobile app companies, and a number of app acquisitions by existing public companies. Previously, many of the companies behind the most popular mobile apps were private companies with closed books, making a full understanding of their data collection practices and business models more difficult.[6] However, an increasing number of app companies are now publicly traded, and therefore subject to the Securities Act of 1933 and the Securities and Exchange Act of 1934.[7] They are required to make certain disclosures to the SEC on a regular basis. In particular, companies must disclose the most significant "risk factors" associated with a company's business. In the current day and age of mobile business, these risks include aspects relating to user data

---

ONLINE PLATFORM ENVIRONMENT 17 (2017) (hereinafter *Online Platform Environment*), https://publications.europa.eu/en/publication-detail/-/publication/04c75b09-4b2b-11e7-aea8-01aa75ed71a1 (citing Néstor Duch-Brown, *The Competitive Landscape of Online Platforms*, JRC TECHNICAL REPORTS (2017), http://ec.europa.eu/jrc/sites/jrcsh/files/ jrc106299.pdf); *see also Commission Inception Impact Assessment on Fairness in Platform-to-Business Relations*, https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-5222469_en (last visited Oct. 16, 2018).

[6] *See* Ilaria Liccardi et al., *Improving Mobile App Selection through Transparency and Better Permission Analysis*, 5 J. PRIVACY & CONFIDENTIALITY 1 (2013) (discussing the technical difficulties with measuring personal information collected by mobile applications); s*ee also* Jinyan Zang et al., *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, TECH. SCI. (Oct. 30, 2015), https://techscience.org/a/2015103001/.

[7] *See infra* notes 49–50.

collection, data privacy, personal information, and the role of, and dependency on, dominant mobile platforms.[8]

Moreover, our approach is informed by recent scholarship on cybersecurity disclosures in SEC filings. This scholarship has mainly focused on the risks to consumer privacy from data breaches,[9] with some using case-study methods to analyze SEC disclosures on cybersecurity,[10] while others have engaged in empirical longitudinal analysis of SEC disclosures on cybersecurity.[11] Privacy scholars have not yet examined SEC disclosures concerning data privacy in mobile app ecosystems. Considering the growing business and financial market implications of privacy governance and regulation,[12] which the SEC has also recognized,[13] we believe

[8] *See infra* notes 11–12 (discussing issues like data privacy and breaches of that privacy).

[9] *See* Joel Bronstein, *The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporation Finance's Recent Guidelines on Cybersecurity Disclosure Requirements*, 13 N.C. J.L. & TECH. ONLINE EDITION 257 (2012); Sam Young, Comment, *Contemplating Corporate Disclosure Obligations Arising from Cybersecurity Breaches*, 38 J. CORP. L. 659 (2013); Mathew F. Ferraro, *Groundbreaking or Broken? An Analysis of SEC Cybersecurity Disclosure Guidance, Its Effectiveness, and Implications*, 77 ALB. L. REV. 297 (2014); Norah C. Avellan, Note, *The Securities and Exchange Commission and the Growing Need for Cybersecurity in Modern Corporate America*, 54 WASHBURN L.J. 193 (2014); and Loren F. Selznick & Carolyn LaMacchia, *Cybersecurity: Should the SEC Be Sticking Its Nose Under This Tent?*, 2016 U. ILL. J.L. TECH. & POL'Y 35 (2016).

[10] *See* Ferraro, *supra* note 9, at 324–35.

[11] *See* Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 173-82 (2005).

[12] *See, e.g.*, Federica Cocco, *Facebook Slides 4% after Cambridge Analytica Revelations*, FIN. TIMES (Mar. 19, 2018), https://www.ft.com/content/66db1ee2-2b57-11e8-9b4b-bc4b9f08f381.

[13] SEC Chairman Jay Clayton, Statement on Cybersecurity, (Sept. 20, 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20 ("Data collection, storage, analysis, availability and protection (including security, validation and recovery) have become fundamental to

SEC disclosure analysis has become an important additional source of information for privacy research (and practice). By analyzing the SEC filings of a select number of public app companies in view of our research question on the relationship between apps and mobile platforms, we also provide evidence on the value of these privacy governance and risk disclosures in SEC filings for privacy research more generally.

The Article is divided into the following sections: Part I introduces the issues relating to privacy in mobile ecosystems, and the current literature on privacy regulation in mobile platforms. Part II then describes and discusses the study undertaken to examine the SEC filings of a set of U.S. public companies that predominantly operate their business, or important parts of their business, as popular apps in the mobile app ecosystem. Finally, Part III provides a discussion on the value of SEC filings for understanding the dependence of mobile apps on mobile platforms for the collection, use and monetization of personal information.

I. BACKGROUND

A. Mobile Privacy

Transparency is a fundamental principle in data privacy regulation, and is particularly important in smartphone ecosystems,[14] given the unique privacy risks associated with mobile devices and mobile applications.[15] However, as

the function and performance of our capital markets, the individuals and entities that participate in those markets, and the U.S. Securities and Exchange Commission.").

[14] *See* Joris van Hoboken et al., Transparency and Privacy in Smartphone Eco-systems: A Comparative Perspective (May 19, 2017) (unpublished manuscript submitted as a draft paper to PLSC Europe) (on file with authors).

[15] *See* FED. TRADE COMMISSION STAFF REP., MOBILE PRIVACY

mentioned above, many of the companies behind the most popular mobile apps have been private companies, and a full understanding of their data collection practices and business models has been difficult.[16] While mobile app companies may provide privacy policies to consumers, these have been found to be vague and ambiguous in terms of setting out a company's data collection and use practices.[17] The privacy-invasive nature of Android and iOS smartphone apps received significant public attention through a report by the *Wall Street Journal* in its influential "What They Know" series.[18] The investigation concluded that "[t]hese phones do not keep secrets. They are sharing [...] personal data widely and regularly."[19] Reports of regulators and studies of privacy disclosures by mobile apps continue to find a lack of transparency toward mobile users, ranging from a complete lack of a privacy policy to more specific omissions in such policies and the use of language that does not properly communicate data processing practices.[20] Effectuating

DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 2, 3 (Feb. 2013); *see also* Jennifer M. Urban, et al., *Mobile Phones and Privacy* (UC Berkeley Public Law Research, Working Paper July 12, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103405.

[16] *See* Liccardi et al., *supra* note 6; Zang et al., *supra* note 6.

[17] *See* Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 85 (2015) (discussing the ambiguity in privacy policy terms); *see also* Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUDIES (SPECIAL ISSUE 2) 2 (2016).

[18] *See* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J., (Dec. 17, 2010), https://www.wsj.com/articles/SB10001424052748704694004576020083703574602.

[19] *Id*.

[20] *See, e.g.*, FEDERAL TRADE COMMISSION STAFF REPORT, *supra* note 15; Article 29 Data Protection Working Party Opinion 00461/13/EN, *Opinion 02/2013 on Apps on Smart Devices* 27 (Feb. 27, 2013), https://www.pdpjournals.com/docs/88097.pdf; EUROPEAN UNION AGENCY FOR NETWORK & INFO. SECURITY, PRIVACY AND DATA PROTECTION IN MOBILE APPLICATIONS, A STUDY ON THE APP DEVELOPMENT ECOSYSTEM

transparency in the mobile context is generally accepted to require a broader perspective than mere privacy policies.[21]

In the U.S. context, the Federal Trade Commission (FTC) has been active in the area of mobile privacy, issuing guidance and recommendations for the industry.[22] The FTC has done so in its role of enforcer of the U.S. consumer protection framework in relation to unfair and deceptive business practices and the Children's Online Privacy Protection Act of 1998 (COPPA), which has been of specific relevance in the area of mobile apps.[23] The FTC has conducted several investigations into the privacy relevant practices of mobile apps, for example its enforcement action against Snapchat.[24] COPPA applies when an app knowingly

---

AND THE TECHNICAL IMPLEMENTATION OF GDPR 19-20 (Nov. 2017); GLOBAL PRIVACY ENFORCEMENT NETWORK, RESULTS OF THE GLOBAL PRIVACY SWEEP 2014 (2014), https://www.dataprotection.ie/docimages/GPEN_Summary_Global_Results_2014.pdf; FUTURE OF PRIVACY FORUM, FPF MOBILE APPS STUDY 2 (2016), https://fpf.org/wp-content/uploads/2016/08/2016-FPF-Mobile-Apps-Study_final.pdf.

[21] *See* Paula J. Bruening & Mary J. Culnan, *Through a Glass Darkly: From Privacy Notices to Effective Transparency*, 17 N.C. J.L. & TECH. 515 (2016).

[22] *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 590-604 (2014) (discussing the role of the FTC in the area of privacy law and policy).

[23] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2012); *see also, e.g.*, Press Release, Fed. Trade Comm'n, Two App Developers Settle FTC Charges They Violated Children's Online Privacy Protection Act (Dec. 15, 2015), https://www.ftc.gov/news-events/press-releases/2015/12/two-app-developers-settle-ftc-charges-they-violated-childrens; Nico van Eijk et al., *Unfair Commercial Practices: A Complementary Approach to Privacy Protection*, 3 EUR. DATA PROTECTION L. REV. 325, 326 (2017).

[24] *See* Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

collects and uses the personal information of children under thirteen years of age. COPPA contains a specific provision on notice (§ 312.4) requiring an app to provide notice and obtain verifiable consent as soon as it collects personal information from children. A recent technical examination of 5,855 Android apps for COPPA compliance found that a majority of these apps were potentially in violation of COPPA as a result of the use of third-party software development kits (SDKs).[25]

Europe has taken a different approach to data privacy regulation than the U.S., anchoring protections in the fundamental rights to privacy and the protection of personal data, and maintaining a broadly applicable legal framework for the processing of personal data by private and public entities.[26] European data privacy law, and the E.U.'s General Data Protection Regulation (GDPR) specifically,[27] has become an increasingly important reference point in U.S. data privacy discussions and practice.[28] The widely discussed GDPR contains a detailed list of transparency obligations concerning the collection and use of personal data, including a right to access one's personal data in Articles 12-15.[29] The E.U.'s ePrivacy Directive contains more specific rules for the

[25] Irwin Reyes et al., "*Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale*, 3 PROC. PRIVACY ENHANCING TECH. 63, 63 (2018).

[26] *See, e.g.*, BART VAN DER SLOOT ET AL., EXPLORING THE BOUNDARIES OF BIG DATA 233 (Bart van der Sloot et al. eds., 2016).

[27] *See generally* Council Regulation 2016/679, 2016 O.J. (L 119) 1 (establishing the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) [hereinafter *General Data Protection Regulation*].

[28] *See, e.g.*, Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO, (Jan. 31, 2018, 12:00 PM), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/; *see also* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 12, 23 (2012).

[29] *See supra* note 27.

electronic communications sector and the tracking of online users.[30] A proposal for a replacement of the Directive by a new Regulation, including rules on privacy settings in browser and operating system software, is under debate in the European Parliament and the Member States.[31]

Reviewing the scientific literature and existing regulatory documents discussed above, the issues at the intersection of privacy and transparency in relation to apps and mobile platforms can be summarized into the following four challenges:

1. The extent to which and the conditions under which applications (obtain) access to personal information on users' smartphones, including through smartphone sensors, and sensitive information stored on or available through the user's device, such as health-related or location data.

2. The lack of transparency about the use and associated privacy implications for mobile users, of third party services, toolkits, libraries and SDKs, for marketing and other purposes, including behavioral advertising, profiling, audience and customer analytics, fraud and security.

3. The lack of and the challenges related to effective transparency about the further use of personal information, including profiling, personalization, artificial intelligence and the sharing of information with third parties.

4. The design of the transparency architecture by the smartphone ecosystem, including the design

[30] *See* Council Directive 2002/58/EC, art. 1, 2002 O.J. (L 201) 42.
[31] *See supra* note 4.

and organization of app stores as well as the design of privacy notifications at installation, notifications during use of applications and the design and availability of settings related to the permissions given to particular applications.

B. Mobile Platforms and Mobile Privacy Governance

Mobile platforms, or perhaps better, mobile ecosystem providers, have obtained a central role in the governance of the collection and use of personal information and the resolution (and creation) of specific data privacy issues. The term mobile platform is used here to refer to the *combination* of app stores and operating system of Apple (iOS) and Google (Android), respectively, offered in the smartphone market. In the case of Apple, the platform for the distribution of applications and the operating system are vertically integrated.[32] In the case of Google's Android (mobile) operating system and Google's platform for getting access to applications, Google Play, the relationship between the two is more complicated.[33] In principle, Android, as an open source operating system, is not directly managed by Google, but by respective mobile device manufacturers, such as Huawei or Samsung.[34] There is some *de facto* vertical integration as a result of non-forking agreements between Google and device manufacturers resulting in the bundling of specific core apps to Android operating system installations (in particular Google Play).[35]

---

[32] Ben Bajarin, *Why Competing with Apple is So Difficult*, Time, http://techland.time.com/2011/07/01/why-competing-with-apple-is-so-difficult/.

[33] *See infra* note 35.

[34] *Id.*

[35] *See* European Commission Press Release IP/16/1492, Antitrust: Commission Sends Statement of Objections to Google on Android

The role of the mobile platforms is a complex one in which the collection and use of user data and related policies play a central role. Eaton et al. have examined the way in which Apple has managed access to specific "boundary resources" for application providers, including the control of customer data and customer privacy.[36] Fong has examined the role of app intermediaries, *i.e.*, the app stores, in protecting data privacy, recommending that the app stores use more of their leverage over apps to ensure respect for data privacy principles. Specifically, Fong suggests that app stores contractually require apps to offer users a right to access their data and abide by other international data privacy principles.[37] There is a large and growing body of computer science literature on mobile privacy, including specific privacy-relevant aspects of the mobile operating system, such as security architectures, privacy permissions and notifications.[38] In addition, user studies document the issues faced by users in understanding the privacy risks

---

Operating System and Applications (Apr. 20, 2016), http://europa.eu/rapid/press-release_IP-16-1492_en.htm; *see also* Kent Walker, THE KEYWORD, Android: Choice at Every Turn (Nov. 10, 2016), https://blog.google/topics/google-europe/android-choice-competition-response-europe/.

[36] Ben Eaton et al., *Distributed Tuning of Boundary Resources: The Case of Apple's iOS Service System*, 39 MIS QUARTERLY 217, 231–33 (2015).

[37] Adrian Fong, *The Role of App Intermediaries in Protecting Data Privacy*, 25 INT'L J. L. & INFO. TECH. 85, 108 (2017).

[38] *See, e.g.,* Serge Egelman, et al., *Choice Architecture and Smartphone Privacy: There's A Price for That*, THE ECON. INFO. SECURITY & PRIVACY 211-36 (Rainer Böhme ed., 2013); Simon Meurer & Roland Wismüller, *APEFS: An Infrastructure for Permission-Based Filtering of Android Apps*, SECURITY & PRIVACY IN MOBILE INFO. & COMMC'N SYS. 1-11 (Andreas U. Schmidt et al. eds., 2012); Ilaria Liccardi et al., *No Technical Understanding Required: Helping Users Make Informed Choices About Access to Their Personal Data*, 2014 PROC. ACM CONF. MOBILE & UBIQUITOUS SYS. 140, 140; Fuming Shih et al., *Privacy Tipping Points in Smartphones Privacy Preferences*, 2015 PROC. ACM CONFERENCE HUMAN FACTORS IN COMP. SYS. 807, 807; *see also supra* note 6.

when using mobile platforms.[39] Greene and Shilton conducted a critical discourse analysis of privacy discussions in Android and iOS developer forums, examining how privacy is defined among mobile application developers, and how mobile platforms, through technical or regulatory means, shape these definitions.[40] Martin and Shilton document the importance of contextual factors for understanding mobile users' privacy preferences and behavior and suggest that common practices in the mobile industry, such as harvesting and reusing location data, images, and contact lists, do not meet users' privacy expectations.[41] In the European context, Loos has examined the contractual relationship between mobile platforms, app developers and consumers.[42] Scholars have also examined the app store review from a freedom of expression perspective.[43]

In view of the power of platforms over other businesses, the European Commission has recently proposed new rules for platforms in an E.U. regulation on fairness and transparency for business users of online intermediation

[39] *See, e.g.*, Jialiu Lin et al., *Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing*, 2012 PROC. ACM CONF. ON UBIQUITOUS COMPUTING; Norman Sadeh et al., *Understanding and Capturing People's Privacy Policies in a Mobile Social Networking Application*, 13 J. PERS. & UBIQUITOUS COMPUTING 401, 402 (2009).

[40] *See* Greene & Shilton, *supra* note 3 (discussing the differences in provider's definition of "privacy" and the ethical implications which arise as a result).

[41] Kirsten Martin & Katie Shilton, *Putting Mobile Application Privacy in Context: An Empirical Study of User Privacy Expectations for Mobile Devices*, 32 INFO. SOC'Y 200, 200, 211 (2016).

[42] Marco B. Loos, *Standard Terms for the use of the Apple App Store and the Google Play Store*, (Ctr. for the Study of European Contract L., Working Paper No. 2016-06 2016).

[43] *See* Luis E. Hestres, *App Neutrality: Apple's App Store and Freedom of Expression Online*, 7 INT'L J. COMM. 1265, 1265 (2013).

services.[44] The proposal seeks to cover app stores, and includes rules on terms and conditions, suspension and termination, ranking, differentiated treatment, complaint handling, and codes of conduct.[45] Notably, Article 7 of the proposed regulation concerns information obligations with respect to how platforms structure access to data that is generated as a result of operating the platform.[46] It provides that mobile platforms "shall include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services."[47] In its preparation for the proposal, the European Commission organized workshops on trading practices between online platforms and business, including on data access, (re-)use and portability in the online platforms environment.[48]

C. SEC Disclosures, Privacy and Information Security

The Securities Act of 1933,[49] and the Securities Exchange Act

---

[44] *See Commission Proposal for a Regulation of the European Parliament and of the Council on Promoting Fairness and Transparency for Business Users of Online Intermediation Services*, COM (2018) 238 final (Apr. 26, 2018).

[45] *Id.* at arts. 3–6, 9–11.

[46] *Id.* at art. 7.

[47] *Id.*

[48] *Commission Report of an Engagement Workshop On Business-to-Business Relationships in the Online Platforms Environment – Data Access, (re-)use and Portability*, at 1 COM (Oct. 19, 2016), https://ec.europa.eu/digital-single-market/en/news/data-related-aspects-business-platform-trading-practices-workshop-report.

[49] 15 U.S.C. §§ 77a–aa (2012).

of 1934,[50] are the main legal instruments regulating the U.S. securities market. The primary purpose of the Securities Act, also known as the "truth in securities" law,[51] is to ensure "full and fair disclosure of the character of securities sold," and to "prevent frauds in the sale thereof."[52] The Securities Exchange Act empowers the SEC to regulate the securities market, and as the SEC states, its main purpose is to ensure that companies publicly offering securities "tell the public the truth about their businesses, the securities they are selling, and the risks involved in investing."[53]

In this regard, public offerings of securities will generally require the company to file a registration statement with the SEC.[54] The registration statement, Form S-1, includes a disclosure document termed a prospectus, and the disclosure requirements in Form S-1 are set out in the SEC's Regulation S-K.[55] The Form S-1 must not only include financial information, such as determining the offering price, but also a detailed "description of business,"[56] any "pending legal proceedings," or "proceedings known to be contemplated by governmental authorities."[57] Moreover, Form S-1 must also include "risk factors," which is a "discussion of the most significant factors that make the offering speculative or risky."[58] In 1998, the SEC adopted a Plain English rule for

[50] 15 U.S.C. §§ 78a–pp (2012).
[51] *The Laws That Govern the Securities Industry*, SEC (Oct. 1, 2013), https://www.sec.gov/answers/about-lawsshtml.html.
[52] 15 U.S.C. § 77 (2012).
[53] *What We Do*, SEC (June 10, 2013), https://www.sec.gov/Article/whatwedo.html.
[54] 15 U.S.C. § 77g (2012); WHITNEY DEBEVOISE & PENNY SOMER-GREIF, SECURITIES LAW IN THE UNITED STATES OF AMERICA, INTERNATIONAL SECURITIES LAW HANDBOOK 503, 503–24 (Jean-Luc & Marcus Best eds., 4th ed. 2005).
[55] 17 C.F.R. § 229.500 (2018).
[56] 17 C.F.R. § 229.101 (2018).
[57] 17 C.F.R. § 229.103 (2018).
[58] 17 C.F.R. § 229.503(c) (2018).

registration statements, which included that risk factors must be written in plain English and "avoid [. . .] 'boilerplate' explanations."[59] Registration statements filed are reviewed by SEC staff, and the SEC will usually issue a comment letter, and the issuer must respond within 30 days, and file an amendment to the registration statement where required.[60] Notably, companies may be subject to criminal and civil liability for "material misstatements or omissions" in offering documents, including by SEC enforcement action.[61]

In addition to filing the registration statement under the Securities Exchange Act, companies that have registered securities for a public offering are required to periodically file an annual report (Form 10-K), a quarterly report (10-Q), and to file a current report (Form 8-K) to disclose certain "material events"[62] (such as bankruptcy, or "other events," for example WhatsApp Inc.'s CEO leaving Facebook Inc.'s board).[63] When a company files a disclosure form with the SEC, the disclosures must conform to the requirements under the SEC's Regulation S-K,[64] and Regulation S-X.[65] The Form 10-K provides a comprehensive overview of the company's business and financial condition and includes audited financial statements, and must also include disclosures regarding a company's business and operations, risk factors, legal proceedings, management discussions and analysis of financial condition and results of operations, financial statements, disclosure controls and procedures, and corporate governance.[66] Importantly, a company's chief

[59] 17 C.F.R. § 230.421(b)(4) (2018).
[60] *See* Debevoise & Somer-Greif, *supra* note 54, at 505.
[61] *Id*. at 510.
[62] *See* Ferraro, *supra* note 9, at 314.
[63] Facebook, Inc., Quarterly Report (Form 8-K) 2 (Apr. 30, 2018).
[64] 17 C.F.R. § 229.1111(h)(4) (2018).
[65] 17 C.F.R. § 210.1-01(a)(1) (2018).
[66] 15 U.S.C. §§ 78m, 78o(d) (2012).

executive officer and chief financial officer must certify the material accuracy and completeness of the disclosures.

In addition to the information expressly required by SEC regulations, a company is required to disclose "such further material information, if any, as may be necessary to make the required statements, in light of the circumstances under which they are made, not misleading."[67] The SEC considers omitted information to be "material" if there is a "substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available."[68] Notably, the SEC has recently adopted new guidance on public company cybersecurity disclosures in February 2018.[69]

Importantly, in addition to SEC enforcement action, which includes criminal and civil penalties, a company may also be sued for damages over material misstatement or omissions in disclosure documents. An example of SEC enforcement action would be Dell Inc.'s agreement in 2010 to pay a $100 million penalty,[70] following an SEC complaint which charged Dell Inc. and its senior executives with filing materially false and misleading annual reports on its Forms 10-K, and materially false and misleading quarterly reports on its Forms l0-Q.[71] Indeed, in April 2018, the company formerly known as Yahoo Inc. paid a $35 million penalty to settle SEC charges that it filed "materially misleading" annual and quarterly reports for failing to disclose a user

[67] 17 C.F.R. § 230.408(a) (2018).
[68] Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8166, 8168 (Feb. 26, 2018).
[69] *Id*.
[70] Dell, Inc., Litigation Release No. 21599, 98 SEC Docket 3272, 3376 (July 22, 2010).
[71] Complaint at 45-46, SEC v. Dell, Inc., No. 10-cv-1245 (RJL) (D.D.C. July 22, 2010).

data breach (affecting 500 million user accounts) for nearly two years.[72] Further, an example of an investor suit would be the class action complaint filed in *Yuan v. Facebook Inc.* in March 2018 in response to the Cambridge Analytica scandal.[73] The suit alleged that Facebook Inc. violated the Exchange Act by making "false and/or misleading statements" in its disclosures, including failing to disclose "Facebook violated its own purported data privacy policies by allowing third parties to access the personal data of millions of Facebook users without the users' consent."[74] The class action followed reporting by *The New York Times* and *The Observer* of London that the voter-profiling company Cambridge Analytica had "harvested private information from the Facebook profiles of more than 50 million users without their permission,"[75] with the investors claiming to have "suffered significant losses and damages" following the decline in the market value of Facebook Inc.'s shares after the revelations.[76] In light of the scandal, it was reported that the SEC had opened an investigation into whether Facebook

---

[72] Altaba, Inc., Release No. 10485 at 9-11 (Apr. 24, 2018), https://www.sec.gov/litigation/admin/2018/33-10485.pdf; Press Release, SEC, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Apr. 24, 2018), https://www.sec.gov/news/press-release/2018-71.

[73] Complaint at 2, Yuan v. Facebook, Inc., No. 5:18-CV-01725 (N.D. Cal. Mar. 20, 2018).

[74] *Id.*

[75] Matthew Rosenberg et al., *How Trump Consultant Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; Carole Cadwalladr & Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, THE GUARDIAN (Mar. 17, 2018, 6:03 PM), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[76] Complaint at 4, Yuan v. Facebook, Inc., No. 5:18-CV-01725 (N.D. Cal. Mar. 20, 2018).

Inc. had adequately disclosed to investors the risks associated with third parties accessing user data without consent.[77]

II. A STUDY ON THE SEC FILINGS OF MOBILE APP COMPANIES

To understand the dependence of mobile apps on mobile platforms, we conducted a study of the SEC filings of a set of U.S. public companies that predominantly operate their business, or important parts of their business, as a popular app in the mobile app environment. We constructed our selection of popular apps developed by publicly-traded companies on the basis of publicly available lists of top free, paid and grossing apps in the U.S. market.[78] The companies

[77] Dave Michaels & Georgia Wells, *SEC Probes Why Facebook Didn't Warn Sooner on Privacy Lapse*, WALL ST. J. (July 12, 2018, 3:00 PM), https://www.wsj.com/articles/sec-probes-why-facebook-didnt-warn-sooner-on-privacy-lapse-1531422043.

[78] *See* Table 1 in the article. In order to make this selection, we first compiled a chart of popular apps for each mobile ecosystem on the basis of publicly available lists of the top free, paid, and grossing apps that were available in Apple's App Store, and Google Play store, on February 20, 2018. The first app owned by a U.S. public company (or a subsidiary) from the first list of these two charts of apps (Apple's App Store) was selected, *e.g.* Bitmoji (Snap, Inc.). Then the first app owned by another U.S. public company (or a subsidiary) from the first list of the second of these two charts (Google Play store) of apps was selected, *e.g.* Instagram (Facebook, Inc.) was selected. This method was repeated until a list of 10 U.S. public companies was reached. Given that a main purpose of the study was to see whether there is a dependence by mobile apps on mobile platforms, it was decided to examine Alphabet, Inc. and Apple, Inc. separately, and thus both these companies are not included in the list. Further, Amazon.com, Inc. and Microsoft Corporation were also not included, as an examination of their SEC filings revealed their mobile apps do not feature prominently. *See also* Amazon.com, Inc., Annual Report (Form 10-K) (Feb. 2, 2018); Microsoft Corp, Annual Report (Form 10-K) (Aug. 2, 2017).

selected are included in Table 1, along with each company's IPO date.

TABLE 1: LIST OF PUBLIC COMPANIES EXAMINED

PUBLIC COMPANY	**POPULAR APPS (AND OTHER APPS OFFERED)**	**IPO**
Snap Inc.	Snapchat, Bitmoji	2017
Facebook Inc.	Facebook, Instagram, WhatsApp, Messenger	2012
Twitter Inc.	Twitter (Periscope)	2013
Match Group Inc.	Tinder, OkCupid, PlentyOfFish	2015
Pandora Media Group Inc.	Pandora Music, Pandora Premium	2011
Zynga Mobile Inc.	Zynga Poker, FarmVille,	2011
Glu Mobile Inc.	Taylor Swift, Kim Kardashian	2007
Activision Blizzard Inc.	Candy Crush Saga, Hearthstone	1993
Electronic Arts Inc.	Star Wars: Galaxy of Heroes, SimCity BuildIt	1989
Take-Two Interactive Software Inc. [79]	Grand Theft Auto, Dragon City, Monster Legends	1997

While the list of U.S. public companies for the study captures some of the most popular and top grossing apps in the Apple and Google mobile ecosystems, it should be noted that focusing on U.S. public companies to examine SEC

[79] TAKE-TWO INTERACTIVE SOFTWARE INC., INVESTOR RELATIONS: CORPORATE PROFILE, http://ir.take2games.com/phoenix.zhtml?c=86428&p=irol-irhome (last visited Oct. 18, 2018).

filings means some popular mobile apps will not be covered. First, there are successful apps developed by U.S. private companies, such as Uber (Uber Technologies Inc.), and Pokémon Go (Niantic Inc.). Second, there are apps developed by non-U.S. public and private companies, such as Angry Birds (Rovio Entertainment Oy, Finland), Super Mario Run (Nintendo Co., Ltd., Japan), and Clash of Clans and Fortnite (Tencent Holdings Ltd., China). Further, the study does not examine apps by public companies that do not feature in the top-end of app store lists of popular apps, like the NYTimes app (The New York Times Company). Of course, some of the private and non-US companies may at some point become publicly-traded in the U.S., like Spotify (Spotify Technology S.A., Luxembourg), which became a "foreign private issuer" in March 2018.[80]

The next stage in the study design was selecting the SEC filings to be examined. As mentioned above, there are three main types of regular filings made to the SEC by public companies, namely the annual Form 10-K, quarterly Form 10-Q, and current Form 8-K; in addition to the registration statement (Form S-1), which is filed when a company makes its IPO.[81] The page length of these filings can be considerable. For example, when Twitter Inc. launched its IPO in 2013, its Form S-1 was 810 pages.[82]

Similarly, Twitter's 2017 annual filing (Form 10-K) was 115 pages, its 2017 fourth quarterly (Form 10-Q) was 75 pages, while its eight current reports in 2017 (Form 8-K) averaged 30 pages each. Thus, to examine all filings made

[80] Spotify Technology S.A., Registration Statement (Form F-1) 52 (Feb. 28, 2018); Ben Sisario & Matt Phillips, *Spotify's Wall Street Debut Is a Success*, N.Y. TIMES (Apr. 3, 2018), https://www.nytimes.com/2018/04/03/business/media/spotifys-wall-street-debut-is-a-success.html.

[81] *See supra* Part I.C.

[82] Twitter, Inc., Registration Statement (Form S-1) (Oct. 3, 2013), https://investor.twitterinc.com/node/8226/html.

with the SEC would have been considerably time-consuming, and it was therefore decided to develop the following methodology. First, each company's Form S-1 was examined, as this filing contains the most elaborated business model description, and how a company might monetize personal information. Second, each company's latest Form 10-K was examined, from which we worked backwards by year, examining each 10-K filing until 2008,[83] or when the company went public (a majority of the companies examined went public after 2008), to see whether there had been changes relating to mobile platform governance changes.

The SEC filings were examined with respect to four issues: (a) the stated role of user data in the company's business model; (b) the stated role of data analytics in the company's business model; (c) the stated dependency on mobile platforms; and (d) the stated risks associated with privacy regulation.

A. Monetization of User Data

By examining the SEC filings across all the companies in the study, our first result is that the monetization of user data, and personal information in particular, is central to the business model of all the companies. Specifically, we found two business model variations within this monetization of user data model. The first variation is an advertising model, which is mainly used by Twitter Inc., Facebook Inc., Snap Inc., and Pandora Media Inc. The second variation is an in-app purchasing model, which is mainly used by Match Group Inc., Zynga Inc., Glu Mobile Inc., Activision Blizzard Inc.,

[83] *See* Dan Rowinski, *History of Mobile App Stores*, READWRITE (Feb. 6, 2012), https://readwrite.com/2012/02/06/infographic_history_of_mobile_app_stores/ (stating that in 2008, both Apple, Inc. (App Store) and Google, Inc. (Android Market) opened their mobile platforms to developers).

Electronic Arts Inc., and Take-Two Interactive Software Inc.

The crucial role of user data in the advertising model comes across clearly in the SEC filings of Twitter Inc., Facebook Inc., Snap Inc., and Pandora Media Inc. For example, for Twitter Inc., mobile advertising represented nearly 90 percent of Twitter's total advertising revenue in 2017, which was $2.4 billion.[84] Twitter derives the majority of its advertising revenues from three products, which are Promoted Tweets, Promoted Accounts and Promoted Trends.[85] However, the key factor in this advertising business model is that Twitter enables "our advertisers to target an audience based on a variety of factors," including what Twitter calls a user's "Interest Graph."[86] This Interest Graph "produces a clear and real-time signal of a user's interests, greatly enhancing the relevance of the ads [Twitter] can display for users and enhancing [its] targeting capabilities for advertisers,"[87] including the "location of the user," a user's follow relationships, combined with a "user's activity on our platform, including who the user replies to, what Tweets the user favorites or retweets, links the user clicks,"[88] and what the user tweets about. The centrality of monetizing user data can also be recognized in Twitter's Form S-1, where it states that its "value proposition to advertisers" is its "ability to target ads based on our deep understanding of our users."[89]

Similarly, Facebook Inc.'s SEC filings revealed that 88% of its revenue in 2017, totaling $40.6 billion, was generated from advertising on mobile devices.[90] Similar to

[84] Twitter, Inc., Annual Report (Form 10-K) 42 (Feb. 23, 2018).
[85] *Id*. at 13.
[86] *Id*. at 6.
[87] *Id*.
[88] Twitter, Inc., Registration Statement (Form S-1) 103 (Oct. 3, 2013).
[89] *Id*. at 6.
[90] Facebook, Inc., Annual Report (Form 10-K) 43 (Feb. 1, 2018).

Twitter Inc., the key value for advertisers is Facebook Inc. enabling "marketers to reach people based on a variety of factors including age, gender, location, interests, and behaviors,"[91] in addition to a user's "education, work history, and specific interests that they have chosen to share with us on Facebook or by using the Like button around the web or on mobile devices."[92] Also similar to Twitter Inc.'s "Interest Graph" for advertisers, Facebook Inc. emphasizes that it enables advertisers to use a unique "Social Context" to enhance the value of ads, which is "information that highlights a user's friends' connections with a particular brand or business."[93] Finally, Facebook Inc. emphasizes its real-name policy to investors,[94] stating that "authentic identity is core to the user experience on Facebook and users generally share information that reflects their real interests and demographics, we are able to deliver ads that reach the intended audience with higher accuracy rates compared to online industry averages."[95]

Pandora Media Inc., with its Pandora Music app, has a similar advertising business model built upon user data, disclosing in its SEC filings that it enables advertisers "to target and connect with listeners based on attributes including age, gender, zip code, and content preferences

---

[91] *Id*. at 5.

[92] Facebook, Inc., Registration Statement (Form S-1) 76 (Feb. 1, 2012).

[93] *Id*. at 3.

[94] Justin Osofsky & Todd Gage, *Community Support FYI: Improving the Names Process on Facebook*, FACEBOOK, INC. (Dec. 15, 2015), https://newsroom.fb.com/news/2015/12/community-support-fyi-improving-the-names-process-on-facebook/. Facebook's real-name policy has been controversial for its impact on privacy and marginalized communities in particular. *See e.g.*, Emanuella Grinberg, *Facebook 'Real Name' Policy Stirs Questions Around Identity*, CNN (Sept. 18, 2014, 6:52 PM), https://edition.cnn.com/2014/09/16/living/facebook-name-policy/index.html.

[95] Facebook, Inc., Registration Statement (Form S-1) 76 (Feb. 1, 2012).

using multi-platform ad campaigns to target their advertising messages to listeners."[96] Notably, Pandora Media Inc. also discloses that it offers advertisers Pandora Audience Targeting, where "advertising products have access to a set of over 2,000 targeting segments across all of our platforms," including "Pandora's inferred Spanish Speakers and Political Preference proprietary segments . . . targeting capabilities, which leverage listener submitted profile information, enabling advertisers to precisely reach sought-after consumers without needing third-party cookies."[97]

Thus, the advertising business model is built upon the ability to target users based on a variety of a user data such as age, gender, location, interests, friends, education, work history, and behavior. Given the centrality of user data to the advertising business model, it is little wonder that, as Facebook Inc. discloses, any changes which "limit our ability to deliver or target advertising on mobile devices" could "adversely affect" monetization on mobile devices.[98]

While Twitter Inc., Facebook Inc., Snap Inc., and Pandora Media Inc. are mainly based on an advertising model,[99] the remaining companies' business models in our examination are predominantly based on in-app purchases, which also include in-app purchasing of premium features (*e.g.,* Match Group Inc.'s dating app Tinder Plus or Tinder Gold).[100] The first relevant feature of the in-app purchasing

[96] Pandora Media, Inc., Annual Report (Form 10-K) 5 (Feb. 13, 2017).
[97] *Id*. at 6.
[98] Facebook, Inc., Annual Report (Form 10-K) 9 (Feb. 1, 2018).
[99] Companies may also combine an advertising and in-app purchasing model, such as Pandora Media, Inc., with nearly 20% of its revenue generated from subscriptions to its premium Pandora Plus app. *See* Pandora Media, Inc., Annual Report (Form 10-K) 52 (Feb. 16, 2017).
[100] *See A Guide to Tinder: Tinder Plus and Tinder Gold*, TINDER https://www.help.tinder.com/hc/en-us/articles/115004487406-Tinder-Plus-and-Tinder-Gold (establishing that "Tinder Plus and Tinder Gold are in-app subscriptions offering access to premium features such as

model is that while these apps may have a very large number of users, only a very small percentage of users pay, and generate the majority of revenue. For example, Glu Mobile Inc., which develops popular gaming apps, and generating "the majority of [its] revenue from Apple's iOS platform,"[101] discloses in its SEC filings that "the percentage of unique paying players for [its] largest revenue-generating free-to-play games has typically been less than 2%."[102] Similarly, Zynga Inc., which also develops popular gaming apps, had revenues of $861 million in 2017, and 86 million monthly active users. However, it disclosed in its SEC filings that only 2.4% of its monthly users are paying users.[103] Thus, this is flagged as a particular risk, as Zynga Inc. relies "on a small portion of [its] total players for nearly all of our revenue."[104] This means that in order to increase revenue, Zynga Inc. must "attract, retain and increase the number of paying players," and "more effectively monetize" players, and "attract them to [its] other games."[105] This monetization of users is where user data and data analytics comes to the fore in the SEC filings of these companies.

For example, Glu Mobile Inc. discloses that it makes "significant investments" in "proprietary analytics" and "monetization techniques" by "segmenting and learning more about the players of each of [its] franchises and further monetizing our highest spending and most engaged players."[106] Thus, "[Glu Mobile aims] to connect the data, insights and knowledge gained from [its] analytics and

---

Unlimited Likes, Passport to chat with singles anywhere around the world, ... With Tinder Gold, you also get exclusive access to our Likes You feature, which lets you see who likes you before you swipe.").

[101] Glu Mobile, Inc., Annual Report (Form 10-K) 48 (Mar. 9, 2018).

[102] *Id*. at 21.

[103] Zynga, Inc., Annual Report (Form 10-K) 10 (Feb. 20, 2018).

[104] *Id*.

[105] Zynga, Inc., Quarterly Report (Form 10-Q) 31 (July 25, 2012).

[106] Glu Mobile, Inc., Annual Report (Form 10-K) 11 (Mar. 9, 2018).

monetization techniques" to "improve player retention and monetization."[107] Similarly, King Digital Entertainment PLC, which was acquired for $5.8 billion by Activision Blizzard Inc. in 2016,[108] adopts a similar data-driven strategy to user monetization, disclosing that "[s]ophisticated targeting has transformed player acquisition,"[109] and it runs "acquisition campaigns in a highly granular and data-driven way."[110] King Digital Entertainment PLC states that it has "built extensive analytics capabilities and proprietary technology infrastructure" to support "growth and retention of our audience through data-driven marketing and management of our games."[111] It adds that it runs "thousands of discrete campaigns every 24 hours, each with individual target metrics, and all subject to the same target return parameters."[112] In a similar vein, one of Zynga Inc.'s stated "core strengths" is its "[s]ophisticated data analytics," with its "proprietary analytics and expertise in high volume data processing," facilitating increased "engagement by [its] players and generate greater sales of virtual goods."[113]

Thus, the in-app purchasing model, similar to the advertising model, is built upon the ability to effectively engage users through data-driven monetization strategies, specifically converting non-paying users to paying users and optimizing the income from already paying users. Notably, companies primarily employing an in-app purchasing strategy may also choose in the future to use their user data sets in developing a stronger advertising model. For example,

---

[107] *Id*.
[108] Activision Blizzard, Inc., Annual Report (Form 10-K) 3 (Feb. 27, 2018).
[109] King Digital Entertainment PLC, Registration Statement (Form F-1) 83 (Feb. 18, 2014).
[110] *Id*. at 87.
[111] *Id*. at 83.
[112] *Id*. at 81.
[113] Zynga, Inc., Registration Statement (Form S-1) 72 (July 1, 2011); *see also* Zynga, Inc., Annual Report (Form 10-K) 2 (Feb. 20, 2018).

while Match Group Inc. currently derives most of its revenue "directly from users in the form of recurring subscriptions,"[114] it also explains that it has the ability "to monetize through advertising."[115] Thus, advertisers can "reach approximately 59 million" monthly users, and Match Group Inc. offers "advertisers the ability to customize their advertisements based on analytics [it collects] about user interests and behavior."[116]

B. Mobile Platform Dependencies

Our study finds that nine out of the ten companies whose SEC filings we analyzed explicitly highlighted significant dependencies on mobile platforms and associated risks flowing from these dependencies.[117] These dependencies were not uniform. We were able to identify a variety of dependencies on mobile platforms, including the challenge of interoperability of apps with mobile operating systems,[118] interoperability of apps with mobile device hardware,[119]

---

[114] Match Group, Inc., Annual Report (Form 10-K) 5 (Mar. 1, 2018).

[115] Match Group, Inc., Registration Statement (Form S-1) 4 (Oct. 16, 2015).

[116] *Id.*

[117] Take-Two Interactive Software, Inc. is the only company not to note its reliance on mobile platforms, but instead notes its reliance on video game platforms, such as Microsoft, Inc.'s Xbox Live and the Sony Corporation's Sony Entertainment Network. *See* Take-Two Interactive Software, Inc., Annual Report (Form 10-K) 7 (May 24, 2017). This may be explained by the fact that most of its revenue is derived from the "sale of products made for video game platforms . . . ." *Id.*

[118] Twitter, Inc., Annual Report (Form 10-K) 38 (Feb. 23, 2018) ("We are dependent on the interoperability of our products and services with popular devices, desktop and mobile operating systems and web browsers that we do not control.").

[119] *See, e.g.,* Snap, Inc., Annual Report (Form 10-K) 11 (Feb. 22, 2018) (Snapchat depends on effectively operating with mobile hardware, "including but not limited to mobile-device cameras.").

access to app marketplaces,[120] visibility and ranking of app in app marketplaces,[121] mobile platforms' in-app payment systems,[122] delivery of advertising and targeted advertising,[123] use of personal information for advertising,[124] access to mobile device identifiers,[125] access to personal information of users,[126] and use of data analytics software.[127] Indeed, as one company states, mobile platforms govern the "promotion, distribution, content and operation generally" of

[120] *See, e.g.,* Twitter, Inc., Annual Report (Form 10-K) 31 (Feb 23, 2018) ("We rely on application marketplaces, such as Apple's App Store and Google's Play, to drive downloads of our mobile applications.").
[121] *See, e.g.,* Pandora Media, Inc., Annual Report (Form 10-K) 15 (Feb. 26, 2018) ("We . . . compete on the basis of the presence and visibility of our app . . . . The websites and mobile applications of our competitors may rank higher than our . . . app . . . which could draw potential listeners away from our service and toward those of our competitors.").
[122] *See, e.g.,* Match Group, Inc., Annual Report (Form 10-K) 13 (Mar. 1, 2018) ("[P]urchases of these subscriptions and features are required to be processed through the in-app payment systems provided by Apple and, to a lesser degree, Google.").
[123] *See, e.g.,* Zynga, Inc., Annual Report (Form 10-K) 14 (Feb. 20, 2018) ("[O]perating systems controlled by third parties increasingly contain features that allow device users to disable functionality that allows for the delivery of advertising on their devices.").
[124] *See, e.g., id.* at 8 (explaining that a platform provider may "limit the use of personal information for advertising purposes[.]").
[125] *See, e.g., id*. at 14 ("[W]hen Apple announced that UDID, a standard device identifier used in some applications, was being superseded and would no longer be supported, application developers were required to update their apps to utilize alternative device identifiers[.]").
[126] *See, e.g.,* Activision Blizzard, Inc., Annual Report (Form 10-K) 21 (Feb. 27, 2018) (explaining that "business could be negatively impacted" if platform providers change "how the personal information of consumers is made available to developers").
[127] *See, e.g.,* Glu Mobile, Inc., Annual Report (Form 10-K) 53 (Mar. 10, 2017)) ("[W]e rely on the data analytics software that we incorporate into our games to calculate and report the [operating metrics] of our games[.]").

all apps on their platform.[128] In the following paragraphs, we discuss these different types of dependencies observed in the SEC filings in more detail.

First, in relation to the advertising business model, Facebook Inc. discloses that its monetization on mobile devices "depends upon" mobile platform standards "that [Facebook does] not control," and any changes which "limit [its] ability to deliver" or "target" advertising could "adversely affect" monetization on mobile devices.[129] Similarly, Twitter Inc. discloses its reliance on mobile platforms, and that mobile platforms "may make changes" such as "limit [its] use of data to provide targeted advertising."[130] This dependency by companies adopting an advertising business model is particularly pronounced, given that a substantial majority of their revenue is derived from mobile advertising; including "[s]ubstantially all" of Snap Inc.'s revenue, such that an "inability to collect and disclose data" or "target the appropriate audience for advertisements" would "seriously harm our business."[131]

Second, similar to the advertising model, those companies using the in-app purchasing model also disclose significant dependences on mobile platforms related to the monetization of user data. For example, Zynga Inc. discloses its reliance on Apple's App Store and the Google Play store, as 84% of revenue is derived from these platforms, and revenue is generated "primarily through the sale of in-game virtual items."[132] Mobile platforms have "broad discretion" to change and interpret its terms of service and other policies; and notably, if mobile platforms "change how the personal information of its users is made available to application

[128] Zynga, Inc., Annual Report (Form 10-K) 8 (Feb. 20, 2018).
[129] Facebook, Inc., Annual Report (Form 10-K) 10 (Feb. 1, 2018).
[130] Twitter, Inc., Annual Report (Form 10-K) 31 (Feb. 23, 2018).
[131] Snap, Inc., Annual Report (Form 10-K) 12–13 (Feb. 22, 2018).
[132] Zynga, Inc., Annual Report (Form 10-K) 4, 6 (Feb. 20, 2018).

developers on the platform,"[133] this could, as Zynga Inc. states, "adversely affect [its] business, financial condition or results of operations."[134] This emphasis on changes in access to personal information by mobile platforms is also made by Activision Blizzard Inc. It warns that if mobile platforms "change how the personal information of consumers is made available to developers," its business "could be negatively impacted."[135]

Similarly, Glu Mobile Inc.,[136] Electronic Arts Inc.,[137] and Match Group Inc.,[138] all highlight the risks associated with their dependence on mobile platforms, including that Apple and Google have "significant influence over the products and services that [they] offer on their platforms,"[139] and that "Apple and Google can unilaterally change its standard terms and conditions with no prior notice to us,"[140] and have "broad discretion" to "interpret their respective terms and conditions in ways that may limit, eliminate or otherwise interfere with our ability to distribute our applications through their stores."[141] As Match Group Inc.

---

[133] *Id*. at 8.
[134] *Id*.
[135] Activision Blizzard, Inc., Annual Report (Form 10-K) 21 (Feb. 27, 2018).
[136] *See* Glu Mobile, Inc., Annual Report (Form 10-K) 22 (Mar. 9, 2018) ("Apple and Google can unilaterally change its standard terms and conditions with no prior notice to us.").
[137] Elec. Arts, Inc., Annual Report (Form 10-K) 14 (May 24, 2017) (Apple's App Store and Google's Play Store "have significant influence over the products and services that we offer on their platforms.").
[138] Match Group, Inc., Annual Report (Form 10-K) 12 (Mar. 1, 2018) (Apple and Google have "broad discretion" to "interpret their respective terms and conditions in ways that may limit, eliminate or otherwise interfere with our ability to distribute our applications through their stores.").
[139] Elec. Arts, Inc., Annual Report (Form 10-K) 14 (May 24, 2017).
[140] Glu Mobile, Inc., Annual Report (Form 10-K) 22 (Mar. 9, 2018).
[141] Match Group, Inc., Annual Report (Form 10-K) 12 (Mar. 1, 2018).

ominously warns, there is "no assurance that Apple or Google will not limit or eliminate or otherwise interfere with the distribution of [its] applications," and should they do so, "[Match Group's] business, financial condition and results of operations could be adversely affected."[142]

While the preceding paragraphs revealed the level of dependency these companies have with regard to mobile platforms and the governance of personal information, our analysis of their SEC filings also reveals some of the concrete consequences for these companies where mobile platforms have unilaterally made changes to their platforms. Beginning with a notable case documented by Twitter Inc. in its filings in February 2018, it noted that because "a majority of [Twitter's] users access our products and services through mobile devices," it is "particularly dependent" on mobile platforms "in order to deliver . . . products and services."[143] In this regard, Twitter Inc. pointed to the detrimental impact of a change Apple made in 2017 to its mobile browser Safari's integration with third-party applications including Twitter.[144] This change resulted in a "decrease of approximately 2 million [monthly active users] who accessed Twitter by using registered third-party applications when those applications automatically contact [Twitter's] servers for regular updates without discernible user-initiated action."[145] This statement referenced a privacy feature Apple introduced in iOS 11 in 2017 to both its desktop and mobile browser Safari 11.0, called Intelligent Tracking Prevention.[146] Apple's Intelligent Tracking Prevention blocks

[142] *Id*.
[143] Twitter, Inc., Annual Report (Form 10-K) 18 (Feb. 23, 2018).
[144] *Id*.
[145] *Id*.
[146] *See* John Wilander, *Intelligent Tracking Prevention*, WEBKIT (June 5, 2017), https://webkit.org/blog/7675/intelligent-tracking-prevention. *See also* Stephen Wilmot, *Apple Changes Business of Selling Your Browsing Data*, WALL ST. J. (Dec. 24, 2017), https://www.wsj.com/articles/apple-

cross-site tracking by removing "cookies and website data for sites with the ability to track users across-site."[147] Indeed, we cross-referenced this effect on Twitter Inc.'s user numbers by examining the SEC filings of the mobile advertising company Criteo S.A.[148] Criteo S.A. noted that Apple's Intelligent Tracking Prevention "blocks some or all third-party cookies by default on mobile" and "makes it more difficult for third-party providers like Criteo to access data on Safari users."[149] Criteo S.A. disclosed that the change had a "net negative impact" on its revenues in the third and fourth quarters of 2017 of "$1.0 million and $25 million."[150]

A second notable case is related to the situation in which mobile platforms make changes to the possibility to use unique mobile device identifiers to track user behavior and deliver targeted advertising. Zynga Inc. notes that mobile platforms' operating systems "increasingly contain features that allow device users to disable functionality that allows for the delivery of advertising on their devices," and

changes-business-of-selling-your-browsing-data-1514127600.

[147] *What's New in Safari, 11.0*, APPLE DEVELOPER PROGRAM, (last updated Feb. 22, 2018), https://developer.apple.com/library/content/releasenotes/General/WhatsNewInSafari/Articles/Safari_11_0.html#//apple_ref/doc/uid/TP40014305-CH13-SW11 (enhancing user privacy by preventing cross-site tracking).

[148] *See* Criteo S.A., Annual Report (Form 10-K) (Mar. 1, 2018). Criteo S.A. is a marketing technology company with 18,000 clients worldwide, and revenues of $2.2 billion in 2017. *Id.* at 1, 2. It helps "commerce companies and brand manufacturers acquire, convert and re-engage their customers, using shopping data, predictive technology and large consumer reach." *Id.* at 126. *See also* Lara O'Reilly, *Ad Tech Firm Criteo Says Apple's New Ad Tracking Limiter Will Hit Its Revenue; Apple's Intelligent Tracking Prevention Feature Makes it Harder for Ad Firms to Target Users*, WALL ST. J. (Nov. 1, 2017), https://www.wsj.com/articles/ad-tech-firm-criteo-says-apples-new-ad-tracking-limiter-will-hits-its-revenue-1509549445.

[149] Criteo S.A., Annual Report (Form 10-K) 26 (Mar. 1, 2018).

[150] *Id.* at 81.

discloses that if users "elect to utilize the opt-out mechanisms in greater numbers, [its] ability to deliver effective advertising campaigns on behalf of [its] advertisers would suffer," and could cause "[its] business, financial condition, or results of operations to suffer."[151] Zynga Inc. points to when Apple announced that its unique device identifier (UDID)[152] was "being superseded and would no longer be supported, application developers were required to update their apps to utilize alternative device identifiers such as universally unique identifier, or, more recently, identifier-for-advertising, which simplify the process for Apple users to opt out of behavioral targeting."[153]

A third case relates to the recent controversy over the

---

[151] Zynga, Inc., Annual Report (Form 10-K) 14 (Feb. 20, 2018).

[152] *See App Programming Guide for iOS – Supporting User Privacy*, APPLE, INC., (last updated Mar. 27, 2017) https://developer.apple.com/library/archive/documentation/iPhone/Conceptual/iPhoneOSProgrammingGuide/ExpectedAppBehaviors/ExpectedAppBehaviors.html#//apple_ref/doc/uid/TP40007072-CH3-SW2 ("If you have not already done so, stop using the unique device identifier (UDID) provided by the uniqueIdentifier [sic] property of the UIDevice class. That property was deprecated in iOS 5.0, and the App Store does not accept new apps or app updates that use that identifier."). For a discussion on whether Google's equivalent Android ID is "personally identifiable information," *see generally* Ariel A. Pardee, *Yershov v. Gannet: Rethinking the VPAA in the 21st Century*, 69 ME. L. REV. 251 (2017); Daniel L. Macioce, *PII in Context: Video Privacy and a Factor-Based Test for Assessing Personal Information*, 45 PEPP. L. REV. 331 (2018).

[153] Zynga, Inc., Annual Report (Form 10-K) 14 (Feb. 20, 2018). *See also* Sito Mobile Ltd., Annual Report (Form 10-K) 20 (Apr. 2, 2018) ("certain mobile devices allow users to "Limit Ad Tracking" on their devices. Like "Do Not Track," "Limit Ad Tracking" is a signal that is sent by particular mobile devices when a user chooses to send such a signal. While there is no clear guidance on how third parties must respond upon receiving such a signal, it is possible that customers, sellers, regulators, or future legislation may dictate a response that would limit our access to data, and consequently negatively impact the effectiveness of our solution and the value of our services on mobile devices.").

use of "loot boxes" in gaming apps,[154] with Apple consequently changing its App Store Guidelines to require that apps "offering 'loot boxes' or other mechanisms that provide randomized virtual items for purchase must disclose the odds of receiving each type of item to customers prior to purchase."[155] Glu Mobile Inc. noted in its March 2018 SEC filings that "Apple updated its terms of service to require publishers to disclose a player's odds of winning the various items contained within loot boxes."[156] Glu Mobile utilizes loot boxes "in many of its current games and the games it intends to release in 2018,"[157] and is "in the process of complying with Apple's new rules."[158] However, it also disclosed that it did not "currently believe that they will have a material impact on the monetization of [its] games that utilize loot boxes."[159] Notably, Glu Mobile Inc. stated that if Apple changes its "terms of service to include more onerous requirements or if Apple (or Google) were to prohibit the use of loot boxes in games distributed on its digital platform," it would "require [Glu Mobile] to redesign the economies of the affected games and would likely cause [its] revenues generated from these games to decline."[160] Similarly, Zynga Inc. highlighted the risk of Apple's new policy, and that it is "continuing to evaluate how Apple will interpret this revision," and "how this rule may affect [its] business, operations and financial

---

[154] *See, e.g.,* Ben Kuchera, *Apple Adds New Rules for Loot Boxes, Requires Disclosure of Probabilities*, POLYGON, (Dec. 21, 2014, 9:44 AM), https://www.polygon.com/2017/12/21/16805392/loot-box-odds-rules-apple-app-store.

[155] *App Store Review Guidelines—Section 3.1.1 In-App Purchases*, APPLE, INC., https://developer.apple.com/app-store/review/guidelines/ (last visited Oct. 18, 2018).

[156] Glu Mobile, Inc., Annual Report (Form 10-K) 22 (Mar. 9, 2018).

[157] *Id.*

[158] *Id.* at 36.

[159] *Id.*

[160] *Id.*

results."[161] Notably Zynga Inc. flagged the risk and uncertainty about "whether Google, Facebook and other platform providers adopt similar rules."[162]

A fourth case we documented through our analysis concerns mobile platform making changes to rules on in-app rewards for advertising viewing and app installs.[163] A company Glu Mobile, Inc. was specifically affected by these rule changes; the company noted that in 2011 Apple began prohibiting virtual currency-incented advertising offers in games that directed users to download other applications from Apple's App Store in order to complete the offer.[164] Glu Mobile Inc. stated that "[t]hese offers accounted for approximately one-third of [its] revenue during the three months ended September 30, 2011, and [its] inability to use such offers has negatively impacted [its] revenue."[165] In addition, Glu Mobile Inc. also noted in its SEC filings that in 2014 "there were reports that Apple was considering prohibiting certain types of virtual currency-incented video advertising in games that promoted other applications available on the Apple App Store."[166] Glu Mobile Inc. disclosed that "incented video advertisements generate a meaningful percentage of [its] overall revenue, and any prohibition of these advertisements would have had a

[161] Zynga, Inc., Annual Report (Form 10-K) 8 (Feb. 20, 2018).
[162] *Id.*
[163] Jason Kincaid, *Apple Clamps Down On Incentivized App Downloads*, TECHCRUNCH (Apr. 19, 2011) https://beta.techcrunch.com/2011/04/19/apple-clamps-down-on-incentivized-app-downloads/. *See also* Sarah Perez, *Apple Begins Rejecting Apps That Offer Rewards For Video Views, Social Sharing*, TECHCRUNCH (June 9, 2014), https://techcrunch.com/2014/06/09/apple-begins-rejecting-apps-that-offer-rewards-for-video-views-social-sharing/.
[164] Glu Mobile, Inc., Annual Report (Form 10-K) 29 (Mar. 9, 2018).
[165] *Id.*
[166] *Id.*

negative impact on [its] revenue."[167]

A fifth case is related to the use of certain software for tracking advertising metrics. Glu Mobile Inc. stated that in 2014, Facebook Inc., in its capacity as a platform for Facebook apps, had "prohibited HasOffers, whose software development kit [Glu Mobile] had incorporated into [its] games to track advertising metrics, from participating in Facebook's mobile measurement program."[168] It was stated that Facebook asserted HasOffers violated its agreement with Facebook.[169] Glu Mobile said that it removed HasOffers' software development kit from their games and "replaced it with software from a new vendor, which did not adversely impact [its] revenue or operations."[170] Notably, Glu Mobile disclosed that any "similar changes or prohibitions in the future, including any changes by Facebook of its advertising platform, which [it relies] on for a majority of [its] user acquisition activities, could negatively impact [its] revenue or otherwise materially harm [its] business, and [Glu Mobile] may not receive significant or any advance warning of

[167] *Id.*

[168] *Id*. at 22.

[169] *See* Ben Kepes, *Holy Ban Batman - Facebook Takes Privacy Seriously And Bans Sketchy Partner*, FORBES (Feb. 12, 2014, 5:00 PM), https://www.forbes.com/sites/benkepes/2014/02/12/holy-ban-batman-facebook-takes-privacy-seriously-and-bans-sketchy-partner/#25cfc2fb5b5b. *See also* Elizabeth Dwoskin & Tony Romm, *Facebook's Rules for Accessing User Data Lured More Than Just Cambridge Analytica*, WASH. POST (Mar. 19, 2018), https://www.washingtonpost.com/business/economy/facebooks-rules-for-accessing-user-data-lured-more-than-just-cambridge-analytica/2018/03/19/31f6979c-658e-43d6-a71f-afdd8bf1308b_story.html?utm_term=.b9d7d3e0e34a ("In 2014, Facebook blocked two advertising partners, HasOffers and Kontagent, for violating policies on retaining customer data and failing to notify partner companies about their data collection practices.").

[170] Glu Mobile, Inc., Annual Report (Form 10-K) 22 (Mar. 9, 2018).

such."[171]

A sixth case concerns some companies that noted a particular reliance on Facebook Inc., such as Match Group Inc.'s Tinder app, where up until 2017, "users currently register for (and log in to) the application exclusively through their Facebook profiles."[172] Match Group Inc. warned that "Facebook has broad discretion to change its terms and conditions applicable to the use of its platform and to interpret its terms and conditions in ways that could limit, eliminate or otherwise interfere with [Match Group's] ability to use Facebook as an authentication method."[173] Relatedly, Zynga Inc.'s filings in 2014 revealed its dependence on Facebook Inc., noting that 75% of its revenue was derived from Facebook users[174] (in contrast to 2017, with only 12% from Facebook, and 51% from Apple).[175] Zynga Inc. stated that its agreement "obligated [Zynga] to use Facebook Credits as the sole in-game payment mechanism in any games launched on [its] own social gaming network, and entitled Facebook to retain 30% of the stated price for transactions on [Zynga's] network."[176] Further, Zynga Inc. disclosed that it was "limited in [its] ability to use a Facebook user's friends list and Facebook's communication channels to promote Zynga.com," and "Facebook amended its standard terms of service to prohibit (i) apps on the Facebook canvas from promoting or linking to game sites other than Facebook and (ii) the use of emails obtained from Facebook to promote or link to desktop web games on platforms other than Facebook."[177] Notably, Zynga Inc. was "prohibited from cross-

[171] *Id.*
[172] Match Group, Inc., Annual Report (Form 10-K) 18 (Feb. 28, 2017).
[173] *Id.*
[174] Zynga, Inc., Annual Report (Form 10-K) 6 (Feb. 21, 2014).
[175] Zynga, Inc., Annual Report (Form 10-K) 4 (Feb. 20, 2018).
[176] Zynga, Inc., Annual Report (Form 10-K) 6 (Feb. 21, 2014).
[177] *Id.* at 9.

promoting traffic to games that are offered on platforms other than Facebook from our games on Facebook," and it was "not permitted to use e-mail addresses obtained from Facebook to promote desktop web games that are not on the Facebook platform, subject to certain limited exceptions."[178] In its latest filings in 2018, Zynga Inc. stated its main reliance is now on Apple Inc. and Google's mobile platforms, generating 84% of its revenue.[179]

Beyond these six cases, there are a number of other potential changes by mobile platforms that we identified that are worth briefly listing to further demonstrate the dependency on mobile platforms. These include platforms imposing file size limitations, which may limit the ability of users to download large apps in over-the-air updates,[180] changing app age-ratings methodology,[181] changing fees related to the distribution of app or delivery of ads,[182] and imposing updated software requirements.[183]

---

[178] *Id*.

[179] Zynga, Inc., Annual Report (Form 10-K) 4 (Feb. 20, 2018).

[180] *Id.* at 8 ("platforms also impose certain file size limitations, which may limit the ability of players to download some of our larger games in over-the-air updates."). *See* Sarah Perez, *Apple Bumps Up the Over-the-Air Download Limit for Apps to 150 MB*, TECHCRUNCH (Sept. 20, 2017), https://techcrunch.com/2017/09/20/apple-bumps-up-the-the-over-the-air-download-limit-for-apps-to-150-mb/.

[181] Glu Mobile, Inc., Registration Statement (Form 424B3) 6 (Nov. 7, 2014) ("Most recently, in the second quarter of 2014, Apple changed its game rating methodology which has resulted in all of our games that include gun violence receiving a 17+ rating, which could potentially negatively impact the number of people playing these "shooter" games and the revenues we generate from these games.").

[182] Facebook, Inc., Annual Report (Form 10-K) 10 (Feb. 1, 2018).

[183] Glu Mobile, Inc., Annual Report (Form 10-K) 22 (Mar. 9, 2018) ("Apple informed developers that beginning on February 1, 2015 all new applications, and beginning June 1, 2015 all updates to existing applications, submitted to the Apple App Store must include 64-bit support. Building our games to support 64-bit development has increased the file sizes of our games making it more difficult for players to download

C. Privacy Regulation

We specifically analyzed the disclosures made in relation to privacy regulations in SEC filings to document the growing economic importance of privacy regulations and changes to them. All the companies examined disclosed as risk factors their compliance with laws on privacy and data protection,[184] security,[185] government investigations,[186] regulatory enforcement actions and settlements.[187] This flows from the fact that, as Twitter Inc. and Facebook Inc. explicitly state, laws on privacy, data protection, and personal information "involve matters central to [their] business[es]."[188] In this regard, there were a number of notable disclosures that merit highlighting.

First, a number of companies make disclosures

our games and potentially negatively impacting the number of downloads and active users of our titles, particularly for those games where we are unable to keep file sizes below 150 megabytes.").

[184] Take-Two Interactive Software, Inc., Annual Report (Form 10-K) 8 (May 24, 2017).

[185] Twitter, Inc., Annual Report (Form 10-K) 24 (Feb. 23, 2018).

[186] Facebook, Inc., Annual Report (Form 10-K) 17 (Feb. 1, 2018).

[187] Twitter, Inc., Annual Report (Form 10-K) 10 (Feb. 23, 2018) ("In March 2011, to resolve an investigation into various incidents, we entered into a settlement agreement with the Federal Trade Commission, or FTC, that, among other things, required us to establish an information security program designed to protect non-public consumer information and also requires that we obtain biennial independent security assessments.").

[188] *Id.* at 9 ("We are subject to a number of U.S. federal and state and foreign laws and regulations that involve matters central to our business. These laws and regulations may involve privacy, rights of publicity, data protection[.]"). *See also* Facebook, Inc., Annual Report (Form 10-K) 24 (Feb. 1, 2018) ("We are subject to a variety of laws and regulations in the United States and abroad that involve matters central to our business, including privacy, data protection and personal information, rights of publicity, content, intellectual property, advertising, marketing, distribution, [and] data security[.]").

relating to previous regulatory action taken against the companies over privacy and user data issues, including all three companies mainly operating an advertising business model. For example, Snap Inc. states that in 2015, the Federal Trade Commission (FTC) "resolved an investigation into some of [its] early practices by issuing a final order."[189] The order required that Snap Inc. "establish a robust privacy program to govern how [Snap treats] user data," and during the "20-year term of the order, [it] must complete bi-annual independent privacy audits."[190] It notes that violating these orders "could subject [the company] to substantial monetary fines and other penalties that could seriously harm [its] business."[191] Similarly, Twitter Inc. also discloses regulatory investigations and settlements could cause it to "change [its] business practices in a manner materially adverse to [its] business."[192] It gives the example of a 2011 settlement with the FTC which "required [Twitter] to establish an information security program designed to protect non-public consumer information and also requires that [it] obtain biennial independent security assessments," with the obligations under the settlement agreement remaining in effect until 2031.[193]

Along with Snap Inc. and Twitter Inc., Facebook Inc.'s registration statement (Form S-1), filed in February 2012, also disclosed that it has been subject to "regulatory investigations and settlements," and "[it] expect[s] to continue to be subject to such proceedings in the future," and which could "require [Facebook to] change [its] business practices in a manner materially adverse to [its] business."[194]

---

[189] Snap, Inc., Annual Report (Form 10-K) 17 (Feb. 22, 2018).
[190] *Id.*
[191] *Id.*
[192] Twitter, Inc., Annual Report (Form 10-K) 26 (Feb. 23, 2018).
[193] *Id.*
[194] Facebook, Inc., Registration Statement (Form S-1) 19 (Feb. 1, 2012).

Facebook Inc. pointed to an agreement with the FTC made four months earlier "to resolve an investigation into various practices by entering into a 20-year settlement agreement that, among other things, requires [it] to establish and refine certain practices with respect to treatment of user data and privacy settings and also requires that [Facebook] complete bi-annual independent privacy audits."[195] Facebook Inc. made the same disclosure about the FTC settlement in its Form 10-K in 2013,[196] 2014,[197] and 2015.[198] However, it did not include this disclosure in its Form 10-K in 2016, 2017, nor in February 2018. In March 2018, following reporting by *The New York Times* and *The Observer* of London that a voter-profiling company had "harvested private information from the Facebook profiles of more than 50 million users without their permission,"[199] the FTC confirmed it had again opened an investigation into Facebook Inc.'s privacy practices.[200] Then, in its Form 10-Q filed in late April 2018,[201] Facebook Inc. disclosed it had become subject to FTC and other government inquiries in the U.S., Europe, and other jurisdictions "in connection with the misuse of certain data by a developer that shared such data with third parties in

---

[195] *Id.*; *see also* Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[196] Facebook, Inc., Annual Report (Form 10-K) 12 (Feb. 1, 2013).

[197] Facebook, Inc., Annual Report (Form 10-K) 11 (Jan. 31, 2014).

[198] Facebook, Inc., Annual Report (Form 10-K) 7 (Jan. 29, 2015).

[199] Rosenberg et al., *supra* note 75; *see also* Cadwalladr & Graham-Harrison, *supra* note 75.

[200] Press Release, Fed. Trade Comm'n, Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices (Mar. 26, 2018), https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection.

[201] Facebook, Inc., Quarterly Report (Form 10-Q) (Apr. 26, 2018).

violation of our terms and policies," and enforcement action "could cause [it] to incur substantial costs, expose [it] to unanticipated civil and criminal liability or penalties (including substantial monetary fines), or require [it] to change [its] business practices in a manner materially adverse to [its] business."[202] In addition, a further risk now arose, as Facebook Inc. had been the "subject of intense media coverage involving the misuse of certain data by a developer that shared such data with third parties in violation of [Facebook's] terms and policies," and such negative publicity could have an "adverse effect on the size, engagement, and loyalty of [its] user base and result in decreased revenue."[203]

Second, all the companies disclose risks not only associated with U.S. laws and regulations, but also foreign laws such as the E.U.'s GDPR,[204] which may "significantly affect" their business.[205] In its February 2018 filings, three months before the E.U. law came into effect, Facebook Inc. stated that the law "will apply to all of [its] products and services that provide service in Europe," and includes "operational requirements for companies that receive or process personal data of residents of the European Union that are different than those currently in place."[206] Notably, Facebook Inc. gives two examples of changes that may occur, namely implementing "measures to change [its] service or limit access to [its] service for minors under the age of 16 for certain countries in Europe," and also be "required to obtain consent and/or offer new controls to existing and new users in Europe before processing data for certain aspects of our

[202] *Id.* at 49.
[203] *Id.* at 46.
[204] *See supra* note 27, at 5.
[205] Facebook, Inc., Annual Report (Form 10-K) 16 (Feb. 1, 2018).
[206] *Id.*

service."[207] In its accompanying call to its Form 10-Q filing in April 2018, Facebook Inc. did indicate European monthly and daily users "may be flat to slightly down sequentially in Q2 as a result of the GDPR roll out," but did "not anticipate these changes will significantly impact advertising revenue."[208]

While Facebook Inc. provides some level of specificity regarding changes as a result of the GDPR, Pandora Media Inc. disclosed that the GDPR "will require" implementation of "do not track" mechanisms and "requirements that users affirmatively 'opt-in' to certain types of data collection and use."[209] This could "significantly hinder [its] ability to collect and use data relating" to users. As such, restrictions on Pandora Media Inc.'s ability to "collect, access and harness listener data," or "disclose listener data or any profiles that [it] develop[s] using such data," could limit its ability to stream personalized music content and offer "targeted advertising opportunities to [its] advertising customers," which are "critical to the success of [its] business."[210]

Third, the SEC filings reveal the relationship between regulation and mobile platform governance. For example, and as mentioned above, Apple changed its App Store Review Guidelines in December 2017 concerning loot boxes. Notably, some companies recognized that the changes made would not "have a material impact on the monetization of [its] games that utilize loot boxes."[211] However, while also warning about the risk to its business if Apple adopted "more onerous" requirements, there was also the added risk that various jurisdictions[212] were reviewing "the legality of loot boxes and

---

[207] *Id*.

[208] Facebook, Inc., First Quarter 2018 Results Conference Call (Transcript) 8 (Apr. 25, 2018), https://investor.fb.com/investor-events/event-details/2018/Facebook-Q1-2018-Earnings/default.aspx.

[209] Pandora Media, Inc., Annual Report (Form 10-K) 24 (Feb. 26, 2018).

[210] *Id*.

[211] Glu Mobile, Inc., Annual Report (Form 10-K) 36 (Mar. 9, 2018).

[212] *See id.* (discussing stringent jurisdictions such as Australia, Belgium,

whether they constitute gambling."[213] In particular, if other jurisdictions determine that loot boxes "constitute gambling or they otherwise elect to regulate the use of loot boxes, it could require [these companies] to stop utilizing loot boxes within [their] games that are distributed in such territories, which would negatively impact [their] revenues."[214]

Fourth, the influence of regulatory action concerning mobile platforms, and the consequences for app companies, was also a feature of the SEC filings. For example, COPPA requires companies to obtain parental consent before collecting personal information from children under the age of 13.[215] Glu Mobile Inc. discussed the FTC's settlement with Apple Inc. in 2014 related to in-app purchases made by minors; and in 2016, the FTC's successful lawsuit against Amazon.com Inc., with a Federal District Court granting summary judgment in favor of the FTC, finding Amazon liable for unfairly billing consumers for unauthorized in-app purchases by minors.[216] Glu Mobile Inc. stated that "if [it does] not follow existing laws and regulations, as well as the rules of the smartphone platform operators, concerning privacy-related matters, or if consumers raise any concerns about [its] privacy practices, even if unfounded, it could damage [its] reputation and operating results."[217]

Finally, we found a number of remaining issues related to privacy regulations that were highlighted in the SEC filings. These included (a) warnings that the application of privacy and data protection laws are often being "unclear,"

---

the Netherlands, the United Kingdom, and the states of Hawaii and Washington).

[213] *Id.*

[214] *Id.*

[215] 15 U.S.C. §§ 6501–6502 (2000).

[216] Glu Mobile, Inc., Annual Report (Form 10-K) 20–21 (Mar. 9, 2018); *see also* FTC v. Amazon Inc., No. C14-1038-JCC, 2016 U.S. Dist. LEXIS 55569, at *1–25 (W.D. Wash. Apr. 26, 2016).

[217] Glu Mobile, Inc., Annual Report (Form 10-K) 38 (Mar. 9, 2018).

with "conflicting" interpretations and applications;[218] (b) companies explicitly stating that they are "bound by our public-facing privacy statement," which "sets forth the ways in which we collect, use and share information";[219] (c) risks associated with proposed legislation, such as the E.U.'s proposed e-Privacy Regulation,[220] which will "notably" amend the "rules on the use of cookies";[221] (d) COPPA,[222] with companies such as Zynga Inc. disclosing that compliance involves "significant operational resources" and "significant expenses";[223] and (e) the reliance some companies have on the international transfer of personal information, such as Twitter Inc. disclosing its reliance "on a variety of legal bases to transfer certain personal information outside of the European Economic Area,"[224] including the E.U.-U.S. Privacy Shield,[225] and E.U. Standard Contractual Clauses.[226]

---

[218] *Id.* ("[I]nterpreting and applying data protection laws to the mobile gaming industry is often unclear. These laws may be interpreted and applied in conflicting ways from state to state, country to country, or region to region, and in a manner that is not consistent with our current data protection practices.").

[219] Pandora Media, Inc., Annual Report (Form 10-K) 23 (Feb. 26, 2018).

[220] Match Group, Inc., Annual Report (Form 10-K) 15 (Mar. 1, 2018).

[221] *Id.*

[222] Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6506 (2012).

[223] Zynga, Inc., Annual Report (Form 10-K) 12 (Feb. 20, 2018).

[224] Twitter, Inc., Annual Report (Form 10-K) 25 (Feb. 23, 2018).

[225] Commission Implementing Decision 2016/1250, of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1, 1 (EU).

[226] Twitter, Inc., Annual Report (Form 10-K) 25 (Feb. 23, 2018).

III. MOBILE DEPENDENCIES AND PRIVACY

A. The Value of SEC Filings

First, our findings suggest that in order to understand the actual impact of a change to a mobile platform's data privacy governance, whether imposed by a platform as a result of a policy decision, or as a direct or indirect result of data privacy regulations, SEC filings can provide evidence of the specific impact on a company's business model and data collection practices. Some of the most significant impacts highlighted in the findings included the impact on Twitter Inc. following Apple Inc.'s introduction of allowing mobile users to prevent cross-site tracking, resulting in a decrease of 2 million monthly average users accessing Twitter through third-party applications.[227] Further, the impact of the change for a major mobile advertising company was quantified as having had a "net negative impact" on revenue in the third and fourth quarters of 2017 of "$1.0 million and $25 million."[228]

Second, the SEC findings can also demonstrate whether a privacy governance change may not be considerably effective. For example, app companies recognize the trend of mobile platform software "increasingly" containing features that "allow device users to disable functionality that allows for the delivery of advertising on their devices,"[229] such as Apple's Limit Ad Tracking,[230] and

[227] *Id.* at 18.
[228] Criteo S.A., Annual Report (Form 10-K) 81 (Mar. 1, 2018).
[229] Zynga, Inc., Annual Report (Form 10-K) 14 (Feb. 20, 2018).
[230] *iPhone User Guide For iOS 6.1 Software*, APPLE, INC., 134 (2013), https://manuals.info.apple.com/MANUALS/1000/MA1658/en_US/iphone_ios6_user_guide.pdf ("Restrict or reset Ad Tracking: Go to Settings > General > About > Advertising. Turn on Limit Ad Tracking to prevent apps from accessing your iPhone's advertising identifier. For more information, tap Learn More.").

Reset Advertising Identifier control introduced in iOS 6.[231] However, SEC disclosures reveal difficulties with such mechanisms, with one company noting that while the Limit Ad Tracking is a signal that is sent by particular mobile devices when a user chooses to send such a signal, "there is no clear guidance on how third parties must respond upon receiving such a signal."[232] Further, SEC disclosures can indicate that users choosing to turn these controls on may be low, and only if users "elect to utilize the opt-out mechanisms in greater numbers, [companies'] ability to deliver effective advertising campaigns on behalf of [their] advertisers would suffer."[233] Thus, effectiveness of certain privacy enhancing controls introduced by mobile platforms can be assessed from SEC disclosures, in particular in how such controls may affect an app company's business. This also raises the issue of circumventing mobile platforms controls, and it should be remembered that in 2012, "Google Inc. . . . agreed to pay a record $22.5 million civil penalty to settle [FTC] charges that it misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking 'cookies' or serve targeted ads to those users."[234]

---

[231] *iOS SDK Release Notes for iOS 6.1*, APPLE, INC. (Jan. 28, 2013), https://developer.apple.com/library/content/releasenotes/General/RN-iOSSDK-6_1/index.html.

[232] Sito Mobile, Ltd., Annual Report (Form 10-K) 20 (Apr. 2, 2018) ("[C]ertain mobile devices allow users to 'Limit Ad Tracking' on their devices. Like 'Do Not Track,' 'Limit Ad Tracking' is a signal that is sent by particular mobile devices when a user chooses to send such a signal. While there is no clear guidance on how third parties must respond upon receiving such a signal, it is possible that customers, sellers, regulators, or future legislation may dictate a response that would limit our access to data, and consequently negatively impact the effectiveness of our solution and the value of our services on mobile devices.").

[233] Zynga, Inc., Annual Report (Form 10-K) 14 (Feb. 20, 2018).

[234] Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-

Third, we found evidence that SEC filings tend to reveal more contextual information concerning a company's use of personal information, in particular relating to how data is monetized, than the information contained in a company's privacy policy. For example, Twitter Inc.'s user "Interest Graph," Facebook Inc.'s "Social Context," or Pandora Media Inc.'s "Pandora Audience Targeting," which each company highlights to investors, are not specifically mentioned in company privacy policies.[235] In relation to its "Interest Graph," Twitter Inc. emphasizes how it "produces a clear and real-time signal of a user's interests, greatly enhancing the relevance of the ads [it] can display for users and enhancing [its] targeting capabilities for advertisers."[236] On the other hand, Twitter Inc.'s privacy policy states that it may "make inferences like what topics you may be interested in. . . and personalize the content [it] show[s customers], including ads."[237] In a similar vein, Facebook Inc. emphasizes its real-name policy to investors,[238] stating that as "authentic identity is core to the user experience on Facebook and users generally share information that reflects their real interests and demographics, [Facebook is] able to deliver ads that reach the intended audience with higher accuracy rates compared to online industry averages."[239] In its privacy policy, Facebook Inc. merely states that it does not "share information that personally identifies you," such as a name,

events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[235] *See Data Policy*, FACEBOOK, INC. (Apr. 19, 2018), https://www.facebook.com/about/privacy/; *see also Pandora Privacy Policy*, PANDORA MEDIA, INC. (Oct. 18, 2016), https://www.pandora.com/privacy; *Twitter Privacy Policy*, TWITTER, INC. (May 25, 2018), https://twitter.com/en/privacy.

[236] Twitter, Inc., Annual Report (Form 10-K) 6 (Feb. 23, 2018).

[237] *See Twitter Privacy Policy*, *supra* note 235.

[238] Osofsky & Gage, *supra* note 94.

[239] Facebook, Inc., Registration Statement (Form S-1) 76 (Feb. 1, 2012).

with "advertising, measurement or analytics partners unless you give [Facebook] permission."[240] In 2015, Facebook Inc. explained that its real-name policy was designed to make users "more accountable," and prevent bullying, anonymous harassment, scamming and criminal behavior.[241]

Fourth, our study shows that SEC disclosures may reveal information not included in privacy policies, such as a company's concerns over a mobile platform simplifying the process for users to opt out of behavioral targeting, and should "users elect to utilize the opt-out mechanisms in greater numbers, our ability to deliver effective advertising campaigns on behalf of our advertisers would suffer, which could cause our business, financial condition, or results of operations to suffer."[242] Similarly, a mobile app company's SEC disclosures may reveal specific information cornering problematic data analytics software used, such as Glu Mobile Inc.'s concern over Facebook prohibiting the HasOffers software development kit, which "[it] had incorporated into [its] games to track advertising metrics," and "any similar changes or prohibitions in the future could negatively impact [its] revenue or otherwise materially harm [its] business, and [Glu Mobile] may not receive significant or any advance warning of such changes."[243]

Fifth, SEC disclosures include previous and ongoing regulatory action concerning privacy issues, which may not be included in a company's privacy policy. As such, SEC disclosures are an interesting source of information for privacy law and policy research, providing references to regulatory issues and past and ongoing litigation. For example, Snap Inc. discloses in its SEC filings that the FTC

---

[240] *Data Policy*, FACEBOOK, INC. (Apr. 19, 2018), https://www.facebook.com/about/privacy/.
[241] Osofsky & Gage, *supra* note 94.
[242] Zynga, Inc., Quarterly Report (Form 10-Q) 40 (Oct. 31, 2017).
[243] Glu Mobile, Inc., Annual Report (Form 10-K) 23–24 (Feb. 28, 2017).

issued a final order in 2014, requiring Snap Inc. to "establish a robust privacy program to govern how [it] treat[s] user data," and "complete bi-annual independent privacy audits," under the 20-year order.[244] Snap Inc. also discloses how it entered a 10-year assurance of discontinuance with the Attorney General of Maryland implementing similar privacy practices, including measures to prevent minors under the age of 13 from creating accounts.[245] The FTC complaint included that Snap Inc. misrepresented its data collection practices, and Snapchat transmitted geolocation information from users of its Android app, despite saying in its privacy policy that it did not track or access such information.[246] Snapchat collected iOS users' contacts information from their address books without notice or consent.[247] Snapchat continued to collect this information without notifying or obtaining users' consent until Apple modified its operating system to provide such notice with the introduction of iOS 6.[248] An open question is whether consumers should also be made aware that a company is subject to a 20-year FTC order, and subject to bi-annual privacy audits. This question also raises a point directly related to platform governance: the effect mobile platform changes have in terms of ending certain data collection practices that may later lead to

[244] Snap, Inc., Annual Report (Form 10-K) 17 (Feb. 22, 2018).
[245] *Id*.
[246] Complaint at 5, *In re* Snapchat, Inc., (F.T.C. No. 132-3078), 2014 WL 7495798 at *3.
[247] Press Release, Fed. Trade Comm'n, Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.
[248] *Id.*; *see also What's New in iOS 6.0*, APPLE, INC., https://developer.apple.com/library/content/releasenotes/General/WhatsNewIniOS/Articles/iOS6.html#//apple_ref/doc/uid/TP40011812-SW7 (describing the changes made in relation to data privacy in iOS 6) (last visited Oct. 18, 2018).

regulatory action.

The Snap Inc. example is quite illustrative: the FTC's complaint stated that prior to September 2012, the Snapchat app collected "not only the phone number a user enters, but also, without informing the user, the names and phone numbers of all the contacts in the user's mobile device address book."[249] Thus, the changes Apple Inc. made in September 2012 to its operating system in iOS 6 had a direct effect on the Snap Inc.'s data collection methods, two years before the FTC's final order was adopted.[250] In iOS 6, the operating system required a user's permission before allowing third-party apps access a mobile device's contacts, calendars, reminders, photo library, and location data.[251]

B. Regulating Business-to-Platform Relations

What is the appropriate legal and regulatory response to the growing dependencies of business on mobile platforms? While discussion of this question goes beyond the scope of this Article and will be explored in depth in future work, the European Commission has recently considered the possibility of E.U. regulatory action concerning business-to-platform relations, and noted that "many small" and "some larger" European businesses have "come to depend on platforms," including app stores, that provide "easy access to customers and markets."[252]

---

[249] Complaint at 6, *In re* Snapchat, Inc., (F.T.C. No. 132-3078), 2014 WL 7495798 at *4.

[250] *See* Press Release, Fed. Trade Comm'n, FTC Approves Final Order Settling Charges Against Snapchat (Dec. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat.

[251] What's New in iOS 6.0, APPLE, INC., https://developer.apple.com/library/archive/releasenotes/General/WhatsNewIniOS/Articles/iOS6.html#//apple_ref/doc/uid/TP40011812-SW7 (last updated June 6, 2017).

[252] *Commission Impact Assessment*, *supra* note 5.

The European Commission described this dependency as entailing an "imbalance of bargaining power," which may give "scope for unfair behaviour" by platforms.[253] Following fact-finding by the European Commission in the form of stakeholder workshops,[254] and an industry survey,[255] the Commission indicated that "some" online platforms engage in "harmful trading practices to the detriment of their business users," and identified six issues: (i) non-negotiability of terms and conditions, which may be changed unilaterally and unannounced; (ii) removal of products or services, including unilateral account suspensions without prior notice,[256] and lack of appeal or statement of reasons; (iii) lack of transparency of platforms' practices, notably concerning search and ranking and advertising placements; (iv) platforms may favor their own products or services, or discriminate between different third-party suppliers and sellers, including tying business users to the platforms' exclusive auxiliary services (e.g. payment services or

[253] *Id*.

[254] *See e.g., Report of an Engagement Workshop Hosted by the European Commission*, EUR. COMM'N (Oct. 19, 2016), https://ec.europa.eu/digital-single-market/en/news/data-related-aspects-business-platform-trading-practices-workshop-report (discussing the findings of a workshop organized under Chatham House rule to discuss specific issues related to trading practices between online platforms and their business users).

[255] *Commission Consultation on What is Your Experience in Trading on Online Platforms?*, EUR. COMM'N (Dec. 7, 2016), https://ec.europa.eu/digital-single-market/en/news/what-your-experience-trading-online-platforms ("All provided information and data will be treated as strictly confidential."). *See Online Platform Environment, supra* note 5 (discussing the results of the survey).

[256] *See* Nicolas Jaimes, *Datas de géolocalisation: Apple éjecte plusieurs médias français de l'App Store* [*Geolocation Data: Apple Ejects Multiple French Media from the App Store*], LE JOURNAL DU NET, (Apr. 15, 2018, 2:21 PM) (Fr.) (explaining that a number of French news media apps were removed from the App Store in April 2018 for transmitting user location data to third parties without explicit consent).

advertising exchanges); (v) business users may lack access to, or the ability to transmit or port, certain types of data, both of a personal and non-personal character (e.g. no access to customer contact details, or contractually limited in their ability to use data generated through a specific platform); and (vi) no meaningful or effective redress.[257] The Commission argues that because of business users' increasing dependency on online platforms to reach markets, these platform practices can have "significant direct negative effects" on many European businesses.[258] This may lead to disengagement from online platforms, hamper the ability to reach markets, indirectly harm consumers by limiting product and service choice, and could have significant negative effects on the wider platform ecosystem, including potential new entrant platforms.

Further, in April 2018, the European Commission published a proposal for an E.U. regulation on fairness and transparency for business users of online intermediation services.[259] The proposal seeks to cover app stores, and includes rules on terms and conditions, suspension and termination, ranking, differentiated treatment, complaint handling, and codes of conduct.[260] Notably, Article 7 of the Regulation concerns access to data, and provides that mobile platforms must provide business users with a description of the technical and contractual access to any personal data or other data which consumers provide for the user of the mobile platform, or which is generated through mobile platforms.[261] The European Commission considered that providing "a single, more far-reaching data sharing obligation," was

[257] *Commission Impact Assessment, supra* note 5.
[258] *Id.*
[259] *See supra* note 44.
[260] *See id.* at arts. 3–6, 9–11.
[261] *See id.* at art. 7.

"judged to be disproportionate."[262] In light of this possible legislative action, SEC disclosures can provide additional empirical evidence of such dependencies.

CONCLUSION

In 2011, the SEC's Division of Corporation Finance issued guidance on disclosure obligations relating to cybersecurity risks and cyber incidents, given the "increasing dependence" of public companies on "digital technologies."[263] Because this dependence increased, the risks to public companies associated with cybersecurity also increased, resulting in more frequent and severe cyber incidents, prompting the SEC to issue the guidance.[264] This has been followed by further SEC guidance in 2018 on cybersecurity disclosures.[265] One may argue that, as demonstrated in our SEC filings study, there is now a similar "dependence" of many of the largest public companies not only on digital technologies, but also on user data and mobile platforms.[266] Indeed, the SEC Chairman recently acknowledged that "data collection, storage, analysis, availability[,] and protection. . . . have become fundamental to the function and performance of our capital markets, [and] the individuals and entities that participate in those markets."[267] Given this dependence, the growing business impact of data privacy rules, and in light of recent data privacy scandals involving the standards for apps to access data through online platforms, one may expect the SEC to heighten its scrutiny of or even consider issuing

[262] *Id*. at 8.
[263] SEC. & EXCH. COMM'N., CF DISCLOSURES GUIDANCE: TOPIC NO. 2 CYBERSECURITY (2011).
[264] *Id*.
[265] SEC. & EXCH. COMM'N, COMMISSION STATEMENT AND GUIDANCE ON PUBLIC COMPANY CYBERSECURITY DISCLOSURES (2018).
[266] *See* discussion *supra* Part I.C.
[267] Clayton, *supra* note 13.

guidance on user data and privacy-related disclosures in the future. While there was a concern that detailed disclosures "could compromise cybersecurity efforts,"[268] no such concerns would be applicable to data protection disclosures.

Second, while the Article demonstrates that apps have a considerable dependence on mobile platforms for the collection and use of data,[269] this may not necessarily be a bad thing from a user privacy perspective. Because of the control mobile platforms exercise over access to and monetization of user data, regulatory action taken by or targeted at mobile platforms may be quite effective (e.g. FTC settlement with Apple Inc. over in-app purchases by children). Further, where a mobile platform adopts a policy change in favor of user privacy (e.g. Apple Inc.'s iOS 6), the impact on the app ecosystem is quite pronounced. In contrast, the European Commission has suggested as a policy option of developing "rules on data access and use" to benefit companies dependent on online platforms,[270] to address the concern that "business users to some extent lack access to and/or the ability to transmit or port certain types of data, both of a personal and non-personal character."[271] This included "targeted marketing initiatives," and the "ability to use data generated through a specific platform to improve their activities on other platforms."[272] However, the European Commission recognizes that "the possible increase in transmissions of personal data between different controllers (platforms and business users) must be assessed" in light of data protection regulation.[273] While this approach

[268] SEC. & EXCH. COMM'N., CF DISCLOSURES GUIDANCE: TOPIC NO. 2 CYBERSECURITY (2011).
[269] *Commission Impact Assessment*, *supra* note 5.
[270] *Id.*
[271] *Id.*
[272] *Id.*
[273] *Id.*

of increasing the "transmissions" of data would address the potential anti-competitive effects of dependencies on mobile platforms, it could also increase the risks to data privacy. In other words, policy makers will have to address the same dilemma as faced by the platforms themselves: balancing the interests of data-driven businesses, while reducing the risk to mobile users' privacy.

Finally, while the primary purpose of this Article was to explore evidence of the dependence of mobile apps on mobile platforms for the collection, use and monetization of personal information, the Article also demonstrates that SEC filings are a rich and fertile ground for privacy research more generally. In light of the size and specific organization of SEC filings, they may be an interesting source of information for automated text analysis of privacy issues and developments. Future research could also broaden the scope of the inquiry to examine mobile advertising companies, mobile data analytics companies, and the securities filings of public companies in other jurisdictions.