Loyola Consumer Law Review

Volume 34
Issue 3 *Symposium Issue 2022*

Article 5

2022

Deficiencies in the Disclosures of Privacy Policies and In User Choice

Scott Jordan
University of California, Irvine

Siddharth Narasimhan
University of California, Irvine

Jina Hong
University of California, Irvine

DEFICIENCIES IN THE DISCLOSURES OF PRIVACY POLICIES AND IN USER CHOICE

*Scott Jordan, Siddharth Narasimhan, and Jina Hong**

Abstract

Development of a comprehensive legal privacy framework in the United States should be based on identification of the common deficiencies of privacy policies. We attempt to delineate deficiencies by critically analyzing the privacy policies of mobile apps, application suites, social networks, Internet Service Providers, and Internet-of-Things devices. Whereas many studies have examined readability of privacy policies, few have specifically identified the information that should be provided in privacy policies but is not.

Privacy legislation invariably starts a definition of personally identifiable information. We find that privacy policies' definitions of personally identifiable information are far too restrictive, excluding information that does not itself identify a person but which can be used to reasonably identify a person, and excluding information paired with a device identifier which can be reasonably linked to a person. Legislation should define personally identifiable information to include such information, and should differentiate between information paired with a name versus information paired with a device identifier.

Privacy legislation often excludes anonymous and de-identified information from notice and choice requirements. We find that privacy policies' descriptions of anonymous and de-identified information are far too broad, including information paired with advertising identifiers. Computer science has repeatedly demonstrated that such information is reasonably linkable. Legislation should define these

---

* Computer Science, University of California, Irvine, CA 92697-3435. Webpage: www.ics.uci.edu/~sjordan/.

Siddharth Narasimhan was a M.S. student in the Networked Systems program at the University of California, Irvine.

Jina Hong is a Ph.D. student in the Informatics program at the University of California, Irvine.

categories of information to align with technological abilities. Legislation should also not exempt de-identified information from notice requirements, to increase transparency.

Privacy legislation relies heavily on notice requirements. We find that, because privacy policies' disclosures of the uses of personal information are disconnected from their disclosures about the types of personal information collected, we are often unable to determine which types of information are used for which purposes. Often, we cannot determine whether location or web browsing history is used solely for functional purposes or also for advertising. Legislation should require the disclosure of the purposes for each type of personal information collected.

We also find that, because privacy policies disclosures of sharing of personal information are disconnected from their disclosures about the types of personal information collected, we are often unable to determine which types of information are shared. Legislation should require the disclosure of the types of personal information shared.

Finally, privacy legislation relies heavily on user choice. We find that free services often require the collection and sharing of personal information. As a result, users often have no choices. We find that whereas some paid services afford users a wide variety of choices, paid services in less competitive sectors often afford users few choices over use and sharing of personal information for purposes unrelated to the service. As a result, users are often unable to dictate which types of information they wish to allow to be shared, and which types they wish to allow to be used for advertising. Legislation should differentiate between take-it-or-leave it, opt-out, and opt-in approaches based on the type of use and on whether the information is shared. Congress should consider whether user choices should be affected by the presence of market power.

1. INTRODUCTION

The cornerstone of recent privacy regulation, including the European General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), is notice-and-choice. Many studies have examined readability of privacy policies, which has implications for requirements regarding clarity of privacy notices. However, the academic literature contains surprisingly few papers that have examined the content of privacy policies, which has implications for the required elements of privacy policies.

In this paper, we analyze the contents of a variety of privacy policies of mobile apps, application suites (e.g. those provided by Google, Microsoft, and Apple), social networks, Internet Service Providers, and Internet- of-Things devices. Our analysis focusses on the collection, use, and sharing of personal information, and on the choices that users are afforded over collection, use, and sharing.

With respect to *collection* of personal information, we ask: What categories of personal information are collected? What types of personal identifiers are used to collate personal information with users? What categories of user behavior do businesses collect, and how do they link this behavior to users? Do businesses assert that this collected information is personally identifiable or anonymous?

We find that businesses collect a wide range of behavioral information. They almost always collect personal information about a consumer's usage of the business's service or app, and the device on which it is run. However, they also often collect personal information about other apps and other devices used by a consumer, whether by observing usage of their app store or by promiscuously sniffing around a user's device and home network. They also often collect personal information about a consumer's interests, whether by observing usage of the service or app, searches, or browsing activity. A limited number of businesses also have the ability to collect personal information about the sites you visit on the Internet. Collection of user location is widespread. Certain types of services and apps also collect content created by users, including files and email. Some also collect audio, video, and sensor data. Some collect information about the people with whom you communicate, and some even collect the content of those communications. Businesses collect a wide range of personal identifiers to collate this information, including a large number of user and device identifiers, advertising identifiers, and sometimes contact information. Assertions of anonymity very often exceed technical reality.

With respect to *use* of personal information, we ask: How is personal information used? What categories of personal information are required to offer a service or app? What categories are not required, but enable additional functionality? What categories are collected to enable behavioral advertising? What other uses are disclosed?

We find that service-related uses of personal information are numerous. Often, personal information is required to offer basic functionality of the service or app. User interests are required to provide search results. The identities of people with whom you communicate are required to deliver email. Cloud storage requires access to files.

Voice assistants often require at least short-term collection of audio. Personal information is also often used to offer additional functionality. Sometimes, information about other apps and devices are used to support communications between multiple apps and devices. Information about a user's interests are very often used to customize the service or app. Location data is almost always used to support location-based services.

Non-service-related uses of personal information almost always focus on advertising. It is often difficult to determine which types of personal information are used for which purposes, and it is particularly difficult to determine which types are used for advertising. Often, personal information is collected that has no apparent use for supporting the service or application, but is likely *only* used for advertising.

With respect to *sharing* of personal information, we ask: With which types of third parties is personal information shared? Do privacy policies disclose which categories of personal information are shared? Do they disclose the purposes for which personal information is shared?

We find that disclosures about sharing of personal information with third parties are limited in detail. Beyond user-directed sharing and sharing for purposes of outsourcing certain business tasks under contract, sharing with third parties is almost always for advertising. However, it is usually difficult to determine which personal information is shared. Sometimes, it appears that the personal information shared principally consists of a combination of a personal identifier and an audience segment used to classify a user interest. However, sometimes it appears that more detailed personal information about a user, including detailed user behavior and location, is shared with third parties without contractual limits on how this personal information is used.

With respect to *user choice* over collection, use, and sharing of personal information, we ask: What types of choices are users afforded? Is it a take-it-or-leave-it proposition? Can users individually determine particular uses of their personal information? Can users prohibit sharing of personal information for particular uses? Does the amount of user choice depend principally on whether the service is paid or free?

We find dramatic differences in user choice practices. Some service or apps give users extensive choices over which of their personal information is collected, while others offer no choices at all. Some services or apps that give users few or no choices over *collection*

of personal information nevertheless give them extensive choices of how this personal information is *used.* And some service or apps that give users few or no choices over either *collection* or *use* give them granular choices over the purposes for which this personal information is *shared* with third parties.

The methodology that we adopt for this paper is to manually inspect a relatively small number of privacy policies in great depth. As we survey in Section 3, there is a spectrum of research approaches to the analysis

of privacy policies. Some papers are based on an automated analysis of thousands of privacy policies, while others are based on a manual inspection of tens of privacy policies. There is a clear trade-off. Automated analysis can examine a large number of privacy policies, but it can inspect only those aspects that can be expressed in formal logic, and it cannot take full advantage of the expertise of knowledgeable privacy researchers. In contrast, manual analysis can examine only a relatively small number of privacy policies, but it can inspect aspects that are regulated by privacy laws in a manner that cannot be expressed in formal logic, and it can take full advantage of the expertise of knowledgeable privacy researchers. We adopt the latter approach here, but view these two approaches as complementary.

Given our approach, we chose the apps and services to analyze to cover what we view as among the most important categories: mobile apps, application suites, social networks, Internet Service Providers, and Internet-of-Things devices. Within each category, we chose three apps or services. Within the category of advertising-supported mobile apps, we chose three popular apps with very different functionality (travel, weather, and real estate). Similarly, with the category of mobile apps for paid services, we chose three popular apps with very different functionality (banking, ride-sharing, and travel). In all other categories, we chose the most widely used services.

Our methodology only considers disclosures in privacy policies. Of course, there are other research approaches that may answer some of the questions we pose above. In particular, a number of academic papers examine the collection and sharing of personal information either by code and/or network traffic. Again, we view these approaches as complementary to the analysis of privacy policies. Examination of code and/or network traffic can illustrate what apps or services actually do, but can rarely determine the purposes for collection, use, and sharing of personal information.

We consider privacy policies that we accessed in California, and that apply in the United States. Although worthy of further study, we did not consider privacy policies specific to other parts of the world.

The paper proceeds as follows. In Section 2, we provide a brief summary of the notice and choice requirements in the GDPR and in the CCPA. In Section 3, we provide an overview of the academic literature on privacy policies.

In Sections 4-9, we attempt to answer these questions about collection, use, sharing, and user choice for providers of a variety of popular categories of services and apps. In each such category, we analyze the privacy policies of a few providers. Section 4 examines advertising-supported mobile apps, while Section 5 examines mobile apps for paid services. We are particularly interested in whether the privacy practices differ based on whether the app is primarily advertising-supported. Section 6 examines the application suites offered by Google, Microsoft, and Apple. We are interested in how much broader the collection, use, and sharing practices are of such application suites than those of mobile apps, based on the breadth of the information available to these suites. Section 7 examines the dominant social network provider, Facebook. We are particularly interested in whether Facebook's privacy practices are similar to those of Google, the other dominant advertising platform. Section 8 examines Internet Service Providers (ISPs). We are particularly interested in whether ISPs have a superior ability to collect personal information, based on their view of the sites you visit on the Internet, or whether they have an inferior view compared to the dominant advertising platforms. Section 9 examines Internet-of-Things (IoT) devices. We are interested in whether IoT devices have unique collection, use, and sharing practices, due to the nature of these devices.

Finally, in Section 10, we ask: Do privacy practices differ principally between different categories of businesses? Do they differ substantially among businesses within the same category? We find that businesses differ in privacy practices based on which online behavior they are able to observe, on their technical sophistication, and on their apparent interest in monetizing personal information. Some businesses collect personal information almost exclusively to provision their service, while others collect substantial amounts of personal information unrelated to the service (often for unrelated advertising). Sharing practices are very diverse, with some businesses selling personal information, some sharing personal information to earn ad revenue, and

others only sharing personal information to outsource service-related tasks.

There are large differences in collection and use for service-related purposes between different categories of service and apps. All categories of services and apps collect personal identifiers, service or app usage, location, and user interests. However, only some categories of services and apps have the technical ability to collect information about other apps and devices, to track widely the sites you visit on the Internet, to collect content, to track communications, and to collect audio, video, or sensor data.

There are large differences in collection and use for advertising purposes, both between different categories and within each category. Because only some categories of services and apps have the technical ability to collect certain type of personal information (e.g., browsing history, content, or communications), only businesses within those categories also use such personal information for advertising. However, we also find that business privacy practices for advertising differ substantially within each category, with some focused mainly on sharing audience segments and others using fine-grained user interests, user content, communications, and perhaps browsing history.

2. CONSUMER PRIVACY LAW & REGULATION

Two recent consumer-oriented privacy laws and regulations—the European General Data Protection Regulation (GDPR)[1] and the California Consumer Privacy Act (CCPA)[2] — include requirements on the content of privacy policies.

Both the GDPR and the CCPA apply to a wide range of businesses. However, in this paper, we focus on online businesses. In the GDPR and in the CCPA, a principal characteristic of a *business* is that

---

[1] European Parliament and Council, General Data Protection Regulation, Regulation (EU) 2016/679 (as amended) (GDPR), April 27 2016 (as amended on May 5 2016), https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04.

[2] California Legislature, California Consumer Privacy Act of 2018 (as amended) (CCPA), June 28, 2018, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4, as amended by the California Privacy Rights Act of 2020, Nov. 3, 2020, https://www.oag.ca.gov/system/files/initiatives/pdfs/190021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

it determines the purposes and means of the processing of consumers' personal information.[3]

The requirements on privacy policies within the GDPR and the CCPA focus on collection, use, and sharing of *personal information*.[4] Personal information includes both (a) personal identifiers and (b) information relating to a person that is either *already linked to* a personal identifier or is *reasonably linkable to* a personal identifier using other reasonably available information.[5] However, the GDPR and the CCPA differ significantly in their definitions, and this may affect the scope of personal information covered under each regulation. We discuss this below when analyzing privacy policies.

In this paper, we focus on the content of privacy policies regarding the *collection*, *use*, and *sharing* of personal information. Both the GDPR and the CCPA require that privacy policies include particular information about collection, use, sharing, and user consent.

With respect to *collection* of personal information, the CCPA requires a business to disclose the categories of personal information it will collect or has collected.[6] The GDPR similarly requires a business to disclose the categories of personal information it has collected.[7] Neither the GDPR nor the CCPA requires a business to disclose the methods by which it collects personal information.

With respect to *use* of personal information, both the GDPR and the CCPA require a business to disclose the purposes for which it collects personal information.[8]

With respect to *sharing* of personal information, regulations differentiate based on the type of entity with which personal information is shared. If the entity with which personal information is shared may use the shared information in a manner in which it determines the purposes and means of any further processing of consumers' personal information, then this entity is also considered to a *business*.

---

[3] In this paper, we use the term *business* to refer to both what the GDPR calls a *controller* (see GDPR Article 4(7)) and what the CCPA calls a *business (see* CCPA Section 1798.140(d).).

[4] In this paper, we use the term *personal information* to refer to both what the GDPR calls *personal data* (see GDPR Article 4(1)) and what the CCPA calls *personal information* (see CCPA Section 1798.140(v)).

[5] This includes information that could reasonably be linked to a person, even if a personal identifier was not part of the original information.

[6] CCPA Sections 1798.100(a)(1), 1798.130(a)(5)(B)(i).

[7] GDPR Article 15(1)(b).

[8] GDPR Articles 13(1)(c), 14(1)(c); CCPA Section 1798.100(a)(1).

If, on the other hand, the entity with which personal information is shared may only use the shared information for purposes specified by the business sharing the personal information, and may not further share the personal information with other entities, then the entity is treated somewhat differently; we refer to this type of entity with which personal information is shared on a restricted basis as a *service provider.*[9]

Both the CCPA and the GDPR require a business to disclose the purposes for which it shares personal information and the categories of recipients of personal information, for recipients who are either other businesses or service providers.[10] The CCPA requires a business to disclose the categories of personal information shared with either another business or a service provider.[11] It is unclear whether the GDPR has a similar requirement, but we expect that this information would be disclosed as part of the consent requirement discussed below.

The GDPR requires a business to disclose the sources of personal information.[12] The CCPA only requires a business to disclose the categories of sources of personal information.[13] Since neither the GDPR nor the CCPA requires a business to disclose a list of specific recipients which with it shares personal information, a consumer may not through such disclosures determine the further downstream sharing on her personal information. Since the GDPR requires disclosure of the *sources* of personal information, a consumer might be able to track the sharing of personal information back to the entity that originally collected it. However, this requires identification of at least one downstream recipient of that personal information.

With respect to *user choice*, three situations are common. First, a service or app's terms and conditions may specify that use of the service is conditioned on a user agreeing to the collection, use, and sharing of personal information. Second, a service or app may give users a choice over collection, use, and/or sharing of personal information, with the default setting allowing such collection, use, and sharing; this is commonly referred to as *opt-out*. Finally, a service or app may give users a choice, with the default setting prohibiting such

---

[9] CCPA defines the terms *contractor* and *service provider*; see CCPA Sections 1798.140(j),(ag). GDPR defines a similar term *processor*; see GDPR Article 4(8).

[10] CCPA Sections 1798.115(a)(2-3); GDPR Articles 13(1)(e), 14(1)(e), 15(1)(c).

[11] CCPA Sections 1798.115(c)(1)-(2), 1798.130(a)(5)(C)(i)-(ii).

[12] GDPR Article 14(2)(f).

[13] CCPA Section 1798.110(c)(2).

collection, use, and sharing; this is commonly referred to as *opt-in*. The GDPR and the CCPA differ on which choices they allow.

The CCPA allows a business to mandate in the terms and conditions of a service the *collection* and *use* of any personal information it desires, except for sensitive personal information that is necessary to perform the service.[14] However, the CCPA only allows a business to mandate the *sharing* of personal information with *service providers*, and only for a specified list of *business purposes*.[15] The CCPA does not allow sharing of personal information for behavioral advertising without user consent.[16] If a business shares personal information with another *business*, then opt-out consent (at a minimum) is required for consumers who are at least 16 years old[17], and opt-in consent is required for consumers less than 16 years old.[18] For personal information subject to either opt-out or opt-in consent requirements, a business must disclose to consumers in privacy policies their rights and choices.[19]

The GDPR takes a somewhat different approach to user consent. It only allows a business to mandate in terms and conditions collection, use, and/or sharing of personal information that is necessary for the performance of the contract between the user and the business.[20] The necessity requirement is a matter of technological feasibility, not of what the business would like to require. Furthermore, the GDPR does not allow a business to mandate the collection, use, or sharing of any *sensitive* personal information, which is delineated in the regulations.[2121] All other collection, use, or sharing of personal information requires opt-in consent.[2222] For personal information subject to opt-in consent requirements, a business must disclose user choices in its privacy policy.[23]

The CCPA applies to companies that do business in California and that collect personal information of 100,000 or more

---

[14] CCPA Section 1798.121(a).
[15] CCPA Sections 1798.140(j)(1), 1798.140(ag(1), 1798.140(e).
[16] CCPA Section 1798.140(e)(4).
[17] CCPA Section 1798.120(d).
[18] CCPA Section 1798.120(c).
[19] CCPA Sections 1798.120(b), 1798.135(a).
[20] GDPR Article 6(1)(b).
[21] GDPR Article 9.
[22] GDPR Articles 4(11), 6(1)(a).
[23] GDPR Articles 13(2)(c), 14(2)(d).

Californians.[24] The CCPA's notice provisions thus likely apply to all of the services and apps analyzed in this paper. Although many of the privacy policies considered have separate notices specifically for California customers, we presume that the collection, use, and sharing practices are uniform nationwide unless stated otherwise. However, the choices that the CCPA mandates that a business must provide are often only afforded to Californians, and we note that as appropriate below.

The GDPR applies to services offered to people residing in the European Union.[25] Thus, it likely applies to most of the services and apps analyzed in this paper, with the notable exception of the services provided by the ISPs considered here. However, few of the privacy policies considered have separate notices or choices for Europeans.

Both the GDPR and the CCPA also require other disclosures in privacy policies, including consumer rights to inspect[26], correct[27], and delete[28] personal information. The GDPR also includes requirements regarding the detail and clarity of privacy policies.[29] Finally, both the GDPR and the CCPA include requirements that go beyond the content of privacy policies, e.g. data minimization. These additional requirements are outside the scope of this paper, albeit quite deserving of their own analyses.

3. RELATED LITERATURE

A. Content of Privacy Policies

The academic literature contains surprisingly few papers that focus on the content of privacy policies. One recent academic paper that does so for a wide range of businesses is Marotta-Wurgler (2016).[30] The paper presented an analysis of 261 privacy policies to determine to extent to which each complies with 49 different self-regulatory guidelines. Regarding collection of personal information, the

---

[24] CCPA Section 1798.140(d).
[25] GDPR Article 3.
[26] GDPR Articles 12(1), 15; CCPA Section 1798.130(a)(5)(A).
[27] GDPR Articles 12(1), 16; CCPA Section 1798.130(a)(5)(A).
[28] GDPR Articles 12(1), 17; CCPA Section 1798.130(a)(5)(A).
[29] GDPR Article 12(1).
[30] Florencia Marotta-Wurgler, "Understanding Privacy Policies: Content, Self-Regulation, and Markets" (Marotta- Wurgler), *NYU Law and Economics Research Paper No. 16-18,* April 2016, https://ssrn.com/abstract=2736513.

paper found that most privacy policies disclosed that the business collected personal identifiers (e.g., a consumer's contact information or IP address)[31] and personal information about consumer behavior (e.g., browsing history or search history)[32]. However, it also found that only a minority of privacy policies disclosed collection of geolocation information other than a consumer's IP address.[33] Regarding use, the paper found that most privacy policies disclosed certain uses of personal information (e.g., behavioral advertising)[34], but that most did not comply with 2012 FTC guidelines regarding disclosures about use[35]. Regarding sharing, the paper found that most privacy policies disclosed that the business shares personal information with third parties[36], but most fail to identify these third parties[37]. It also found that only a small proportion disclosed that sharing is subject to a contract with third parties establishing how recipients may use this personal data.[38] Regarding user choice, the paper found that many privacy policies gave users some ability to adjust privacy settings[39], but that most privacy policies do not give users choice over sharing of personal information[40]. In summary, the paper found that most privacy policies did not comply with most of the 2012 FTC guidelines.[41] However, it also found significant differences in compliance both between and within markets.[42]

The Global Privacy Enforcement Network, an informal network of European government agencies tasked with enforcement of privacy laws and regulations, conducted an examination of privacy policies in 2017 and briefly summarized their findings in a report.[43] The report documented whether it was clear from the perspective of a consumer what personal information is collected, how it is used, and

---

[31] Marotta-Wurgler at 21 and at Table 3 N4-N5.
[32] Marotta-Wurgler at 21 and at Table 3 N6.
[33] Marotta-Wurgler at Table 3 N10.
[34] Marotta-Wurgler at Table 3 N15.
[35] Marotta-Wurgler at Table 3 N13.
[36] Marotta-Wurgler at Table 3 SH5.
[37] Marotta-Wurgler at 21 and at Table 3 N16.
[38] Marotta-Wurgler at 21 and at Table 3 SH7.
[39] Marotta-Wurgler at 22 and at Table 3 UC1.
[40] Marotta-Wurgler at 22 and at Table 3 SH8.
[41] Marotta-Wurgler at 30-31.
[42] Marotta-Wurgler at 25-28 and at Table 5.
[43] Global Privacy Enforcement Network, GPEN Sweep 2017 'User Controls over Personal information' (GPEN), *UK Information Commissioner's Office*, October 2017, http://www.astrid-online.it/static/upload/2017/2017-gpen-sweep-international-report1.pdf.

how it is shared. The report generally found that privacy policies lacked detail.[44] With respect to collection, the report found that most privacy policies disclosed what personal information is collected, including personal identifiers (e.g., name, address, phone number, or email address) and personal information about consumer behavior (e.g., usage data or location).[45] With respect to sharing, the report found that about half of the privacy policies examined failed to specify with whom personal information is shared, and about a quarter failed to specify whether personal information is shared at all.[4646]

Recently, Linden et al. (2020) examined how privacy policies changed from January 2016 (pre-GDPR) to May 2019 (post-GDPR).[47] The paper examined 6,278 privacy policies, and found that the average length increased from roughly 1,800 words to roughly 2,400 words.[48] The analysis suggests that there was a significant increase in disclosure of user rights, but not necessarily in disclosure about collection, use, and sharing.[49]

The academic literature also contains a few papers that examine the content of privacy policies for specialized industries. Cranor et al. (2015) presented an analysis of 75 privacy policies of online tracking companies to determine whether they contained information relevant for users to make privacy decisions.[50] For purposes of the study, the researchers categorized personal information as either *personally identifiable* (e.g., name or address) or *anonymous* (e.g., characteristics of a consumer that are not accompanied with a personal identifier)[51], and as either *sensitive* (e.g., race, religion, sexual orientation, health condition, or income bracket) or *non-sensitive* (e.g., gender or age).[52]

---

[44] GPEN at 2.

[45] GPEN at 3-4.

[46] GPEN at 5.

[47] Thomas Linden, Rishabh Khandelwal, Hamza Harkous, and Kassem Fawaz, "The Privacy Policy Landscape After the GDPR" (Linden), *Proceedings of Privacy Enhancing Technologies*, vol. 2020 issue 1, 2020, 47-64, https://doi.org/10.2478/popets-2020-0004.

[48] Linden at Table 3.

[49] Linden at 55-56.

[50] Lorrie Faith Cranor, Candice Hoke, Pedro Giovanni Leon, and Alyssa Au, "Are They Worth Reading? An In-Depth Analysis of Online Trackers' Privacy Policies" (Cranor 2015), *I/S: A Journal of Law and Policy for the Information Society*, vol. 11 no. 2, 2015, 325-404, https://kb.osu.edu/handle/1811/75475.

[51] *Id.* at 334.

[52] *Id.* at 336.

We note, however, that such categorizations do not necessarily align with the definitions and treatment of *personal information* under either the GDPR or the CCPA.[53] In particular, what the paper categorizes as *anonymous information* may be categorized by the GDPR or the CCPA as *personal information* if it can be reasonably linked with a personal identifier. With respect to collection, the paper found that most of the privacy policies of online tracking companies disclosed that the business collects anonymous information, and that many disclose whether or not they collect personally identifiable information.[54] However, most privacy policies do not disclose whether they collect sensitive anonymous information, and many do not disclose whether they collect geolocation information.[55] With respect to use, the paper found that most of the privacy policies of online tracking companies disclosed the use of anonymous information for targeted advertising, and that about half disclosed the use of anonymous information for user and advertisement analytics.[56] With respect to sharing, the paper found that most of the privacy policies of online tracking companies disclosed sharing of anonymous information with non-affiliates.[57] It also found that most do not disclose whether they allow recipients to combine the anonymous information with personal identifiers, which would render the information as personally identifiable.[58] With respect to user choice, the paper found that most privacy policies of online tracking companies allow users to opt-out of the use of personal information for targeted advertising, but do not allow users any control over collection, other types of use, or sharing for other purposes.[59] It also found that although most claimed not to merge anonymous information with personal identifiers, those that reserved the right to do so did not give users any choice over the practice.[60]

Kamarinou et al. (2016) presented an analysis of 20 privacy policies of cloud service providers who provide services including file

---

[53] The CCPA excludes *deidentified information* from *personal information*; see CCPA Sections 1798.140(m), 1798.140(v)(3). However, the CCPA's definition of *deidentified information* is considerably more limited than Cranor's definition of *anonymous information*.

[54] Cranor 2015 at Figure 1(a), (c).

[55] *Id.* at Figure 1(b), (d).

[56] *Id.* at Figure 3.

[57] *Id.* at Figure 2(a).

[58] *Id.* at Figure 2(d).

[59] *Id.* at Figure 5(a), (c).

[60] *Id.* at Figure 5(d) and at 350.

storage, video streaming, email, and social networking to determine how the privacy policies treat user rights about collection, use, and sharing of personal information.[61] First, the paper found that privacy policies used a wide variety of often-conflicting definitions of *personal information*, *personally-identifiable information*, *de-identified information*, and *aggregate information*, and warned that the definitions often did not align with those in privacy laws and regulations.[62] With respect to collection, the paper found that most privacy policies of cloud service providers disclose collection and use of both personal identifiers (e.g., name, email address, IP address, or device identifiers) and usage information (e.g., time and location of usage).[63] With respect to use, the paper found that most privacy policies of cloud service providers disclosed use of personal information for purposes of the cloud service[64], and that some disclosed use for targeted advertising[65]. Nevertheless, the paper found that disclosed purposes are not always clear, explicit, specific, or exhaustive.[66] With respect to sharing, the paper found that most privacy policies of cloud service providers disclosed sharing of personal information with third parties.[67] In some cases, they found that recipients were limited in the use of shared information[68], but in other cases they found that cloud service providers claimed not to have any control over the practices of third parties[69].

Cranor et al. (2016) presented an automated analysis of 6,191 privacy policies of U.S. financial institutions to compare the disclosures and consumer choices.[70] With respect to collection, the paper

---

[61] Dimitra Kamarinou, Christopher Millard, and W Kuan Hon, "Cloud privacy: an empirical study of 20 cloud providers' terms and privacy policies – Part I" (Kamarinou), *International Data Privacy Law*, vol. 6 no. 2, 2016, https://watermark.silverchair.com/ipw003.pdf.

[62] *Id.* at 85.

[63] *Id.* at 87-89.

[64] *Id.* at 92.

[65] *Id.* at 90-91.

[66] *Id.* at 93.

[67] *Id.* at 95.

[68] *Id.* at 94.

[69] *Id.* at 95.

[70] Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur, "A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices" (Cranor 2016), *ACM Transactions on the Web*, vol. 10 no. 3, Aug. 2016, https://dl.acm.org/doi/10.1145/2911988.

found that most privacy policies of financial institutions disclose collection of a variety of personal information related to the financial service (e.g., account balance and payment history).[71] With respect to sharing, although the paper found that most financial institutions shared personal information for business purposes, it also found that the privacy policies varied starkly, particularly in terms of whether they share personal information with affiliates.[72] With respect to user choice, the paper found that a minority of financial institutions allowed opt-out of any type of sharing of personal information, and most of those that did so did not provide electronic means for exercising the option.[73] Overall, the paper found that privacy practices varied substantially, even between institutions with similar specializations.[74]

B. Privacy Policy Readability and User Comprehension

In contrast to the scant academic literature on the content of privacy policies, there is a rich academic literature on the readability of privacy policies and on user comprehension.

McDonald and Cranor (2008) estimated the time required to read and to understand privacy policies.[75] First, they examined the privacy policies of the 75 most popular websites. They found that the interquartile range[76] of the length of these privacy policies was approximately 2,000 to 3,000 words, and estimated that it would take a typical user with a high school education 8 to 12 minutes to read such a policy.[77] Second, the researchers conducted an online study that asked 168 participants to skim one of six privacy policies of varying lengths and to find answers to five multiple choice questions about privacy protections (e.g., "Does the website use cookies?").[78] In this situation, the paper found that the interquartile range time to skim privacy policies with interquartile range lengths and answer the five questions was

---

[71] Cranor 2016 at 16.

[72] Cranor 2016 at 13-14.

[73] Cranor 2016 at 14-15.

[74] Cranor 2016 at 17-24.

[75] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies" (McDonald 2008), *I/S: A Journal of Law and Policy for the Information Society*, vol. 4 no. 3, 2008, 543-568, https://kb.osu.edu/handle/1811/72839.

[76] The interquartile range is the 25th to 75th percentiles.

[77] McDonald 2008 at Table 1.

[78] McDonald 2008 at 555.

approximately 15 to 35 minutes, with a median of approximately 23 minutes.[79] The paper also estimated that on average a U.S. Internet user visits approximately 1,462 unique websites annually.[80] Consequently, the paper estimates that a typical user with a high school education would need roughly 40 minutes per day, each day over the course of 1 year, to read (once per year) each privacy policy of websites they visit.[81]

Fabian et al. (2017) presented an automated analysis of the readability of nearly 50,000 privacy policies.[82] The paper found that the length of privacy policies varied widely, with a mean of about 1,700 words in 70 sentences.[83] The analysis calculated a number of established readability measures based on the length and lingual complexity of each policy, and found that on average privacy policy readability was "difficult", although they ranged from "very easy" to "very difficult".[84] It also found that most privacy policies require an education level of high school or some college to be read with ease.[85]

Hoofnagle and King (2008) surveyed 991 Californians about their understanding of the purpose of privacy policies.[86] The paper Illustrated a number of common misconceptions. About half thought that the mere presence of a privacy policy prohibits the sale, or even the sharing with affiliates, of online purchasing information.[87] About 40% thought that the mere presence of a privacy policy mandates disclosure of the recipients of shared personal information[88], and over half

---

[79] McDonald 2008 at Figure 2.

[80] McDonald 2008 at Table 5.

[81] McDonald 2008 at 563.

[82] Benjamin Fabian, Tatiana Ermakova, and Tino Lentz, "Large-Scale Readability Analysis of Privacy Policies" (Fabian), *Proceedings of the International Conference on Web Intelligence*, August 2017, https://dl.acm.org/doi/10.1145/3106426.3106427.

[83] Fabian at 21.

[84] Fabian at 21.

[85] Fabian at 21.

[86] Chris Jay Hoofnagle and Jennifer King, "What Californians Understand About Privacy Online" (Hoofnagle), *draft paper,* April 2016, September 3 2008, https://ssrn.com/abstract=1262130.

[87] Hoofnagle at 12-14.

[88] Hoofnagle at 15.

thought it mandates consumer rights to access, correct, and delete personal information[89].

McDonald et al. (2009) compared the readability and comprehension of layered privacy policies and of standardized privacy policies with that of conventional privacy policies.[90] The paper found that readability slightly increased with both layered and standardized privacy policies over that of conventional policies, but that comprehension of layered policies decreased for topics that were not in the top layer of the policy.[91]

Reidenberg et al. (2014) compared comprehension between users with different levels of privacy knowledge of elements of six privacy policies concerning collection and sharing of personal information.[92] The paper found that even experts often disagreed about the implication of privacy policies; that non-experts often did not perceive the same ambiguity as experts did; and that comprehension often falls off with decreasing knowledge level.

Waldman (2018) surveyed 495 users on their trust of websites based on privacy policies that varied both in data practices and graphic design.[93] The paper found that users who are relatively unknowledgeable of the legal implications of privacy practices often trust websites with invasive privacy policies designed with a modern aesthetic over websites with privacy-protective policies presented in a traditional manner.

---

[89] Hoofnagle at 19-20.

[90] Aleecia M. McDonald, Robert W. Reeder, Patrick Gage Kelley, and Lorrie Faith Cranor, "A Comparative Study of Online Privacy Policies and Formats" (McDonald 2009), *Proceedings of the 9th International Symposium on Privacy Enhancing Technologies,* August 2009, published in *Lecture Notes in Computer Science*, vol. 5672, 37-55, https://link.springer.com/chapter/10.1007/978-3-642-03168-7_3.

[91] McDonald 2009 at 14-15.

[92] Joel R. Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T. Graves, Fei Liu, Aleecia McDonald, Thomas B. Norton, Rohan Ramanath, N. Cameron Russell, Norman Sadeh and Florian Schaub, "Disagreeable Privacy Policies: Mismatches between Meaning and User' Understanding" (Reidenberg 2014), *Berkeley Technology Law Journal*, vol. 30 no. 1, 2014, 39-68, https://btlj.org/2015/10/disagreeable-privacy-policies/.

[93] Ari Ezra Waldman, "A Statistical Analysis of Privacy Policy Design" (Waldman), *Notre Dame Law Review Online*, vol. 93, 2018, 101-112, http://ndlawreview.org/2018/04/a-statistical-analysis-of-privacy-policy-design/.

C. Other Types of Papers on Privacy Policies

In addition to the academic literature on the content of privacy policies and on the readability of privacy policies, there is a rich academic literature that focusses on other aspects of privacy policies. A number of papers examine the choices that users are offered. Habib et al. (2019) examined 150 websites, looking for user controls regarding email communications, targeted advertising, and a user's right-to-delete personal data.[94] The paper found that most of the examined websites offered some type of user choice, and that most of these choices were provided through privacy policies. However, the paper also found that user controls were sometimes difficult to find and/or understand. Utz et al. (2019) examined over 80,000 user visits to one website to determine the influence of various factors on the choices that users made.[95] The paper found that graphical user interface properties and default choices both significantly influenced user choices. Das et al. (2019) conducted an experiment with seven people to study the effect of the relationship between user choices and service functionality on user privacy choices on Facebook.[9696] The paper suggests that increased transparency about the effect of user choices upon the resulting functionality of the service may increase the proportion of users who change default privacy options.

A number of papers propose methods to improve privacy policies. Some papers, e.g. Kelley et al. (2009)[97], propose privacy labels to

---

[94] Hana Habib, Yixin Zou†, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub, "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites" (Habib), *Proceedings of the USENIX Symposium on Usable Privacy and Security*, August 2019, 387-406, https://www.usenix.org/conference/soups2019/presentation/habib.

[95] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field" (Utz), *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, November 2019, 973-990, https://dl.acm.org/doi/10.1145/3319535.3354212.

[96] Sanchari Das, Jayati Dev, and L. Jean Camp, "Privacy Preserving Policy Framework: User-Aware and User-Driven" (Das), *Research Conference on Communications, Information and Internet Policy,* September 2019, https://ssrn.com/abstract=3445942.

[97] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder, "A 'Nutrition Label' for Privacy" (Kelley), *Proceedings of the Symposium on Usable*

standardize the presentation of information regarding the collection, use, and sharing of personal information. Others, notably including a Federal Trade Commission 2012 Report[98], suggest best practices, including elements of transparency and user choice.

4. ADVERTISING-SUPPORTED MOBILE APPS (KAYAK, THE WEATHER CHANNEL, AND ZILLOW)

There are a tremendous number of mobile apps that are primarily supported by advertising. We analyze here three popular apps: Kayak[99] (a travel search app), The Weather Channel[100] (a weather app), and Zillow[101][101] (a real estate app). Our goal is both to compare their collection, use, and sharing of personal information with each other, and to later compare these practices to those of mobile apps that are not primarily supported by advertising and to other types of online services.

A. Scope

Each of the three privacy policies apply to the service's mobile apps and websites.[102] Some policies also apply to other services (e.g., Zillow home buying and mortgage services[103]). We focus here only on the mobile apps.

Some mobile apps are owned by parent companies that operate other services. KAYAK is owned by a parent company whose subsidiaries include booking.com, OpenTable, and Priceline; KAYAK both

---

Privacy and Security, July 2009, Article 4, https://dl.acm.org/doi/10.1145/1572532.1572538.

[98] Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers" (FTC 2012), March 2012, https://www.ftc.gov/reports/protecting-consumer-privacy- era-rapid-change-recommendations-businesses-policymakers.

[99] KAYAK Software Corporation, "Privacy Policy" (KAYAK), July 1, 2020, https://kayak.com/privacy.

[100] The Weather Company, "Privacy Policy" (The Weather Channel), December 29, 2019, https://weather.com/en-US/twc/privacy-policy.

[101] Zillow Group, "Privacy Policy" (Zillow), January 1, 2020, https://www.zillowgroup.com/zg-privacy-policy/.

[102] KAYAK; The Weather Channel; Zillow at "Introduction".

[103] Zillow at "Introduction".

collects personal information from and shares personal information with these other subsidiaries.[104] The Weather Channel is owned by parent company IBM, but it unclear whether The Weather Channel shares personal information with IBM.[105]

B. Collection

As discussed in Section 2, the GDPR and the CCPA require a business to disclose the categories of personal information it collects, but not to disclose the methods by which it collects personal information. All three free apps collect personal identifiers, including device identifiers (e.g., IP address and other unspecified device identifiers) and advertising identifiers (e.g., Apple or Android advertising identifier).[106] The Weather Channel app doesn't collect contact information, but the KAYAK and Zillow apps do (e.g., name, address, email address, phone number) if you login with an account.[107]

All three free apps also collect some behavioral information, including devices used by a consumer (e.g., "[i]nformation about your device and device capabilities"[108]) and app usage (e.g., "[i]nformation about how you use the Services"[109] and "[y]our activities on the Services"[110]).

All three free apps collect behavioral information if the user interacts with an ad (e.g., if a user "[e]ngage[s] with interactive advertising"[111] and "the links you click"[112]). In addition, KAYAK and Zillow have the ability to collect a significant amount of other behavioral information that focusses on user interests, including "information about your [travel] searches"[113], "the type of home or number of

---

[104] KAYAK, *supra* note 99.

[105] The Weather Channel.

[106] KAYAK at "Information We Collect and Use"; The Weather Channel at 1.B; Zillow at "Device information".

[107] KAYAK at "Personal Information We Collect Directly From You"; Zillow at "Information you give us or create using our services".

[108] The Weather Channel at 1.B.

[109] The Weather Channel at 1.B.

[110] The Weather Channel at 1.B.

[111] The Weather Channel at 1.A.

[112] KAYAK at "Usage and performance information".

[113] KAYAK at "Usage and performance information".

bedrooms" of homes you search for[114], "homes you view"[115], and "other software installed on your device"[116]. If you login, KAYAK may collect other personal details about you (e.g., age or birthdate and gender)[117], but Zillow refrains from doing so. If you make travel arrangements, KAYAK may also collect information about your itinerary.[118]

All three free apps also collect information about a user's location, using information provided by mobile devices (e.g., IP address, accessible Wi-Fi and Bluetooth networks, accessible cell towers, and GPS information).[119] The location information typically includes the "latitude and longitude of your mobile device" and "sensor data such as altimeter".[120] The Weather Channel app may also collect "your device's motion data".[121] Location data may be either collected only while using the app or at all times, depending on the privacy setting.[122]

None of these free apps are in a privileged position to observe the behavioral information that they collect, as there are many competing apps with similar functionality.

C. Use

As discussed in Section 2, the GDPR and the CCPA require a business to disclose the purposes for which it collects personal information. Mobile apps differ in how (and even if) they define *personal information.*[123]

---

[114] Zillow at "Home Search".

[115] Zillow at "Activity information".

[116] KAYAK at "Device information".

[117] KAYAK at "Personal details".

[118] KAYAK at "Booking information".

[119] KAYAK at "Location information"; The Weather Channel at 1.C; Zillow at "Location Information".

[120] The Weather Channel at 1.C.

[121] The Weather Channel at 1.D.

[122] KAYAK at "Location information"; The Weather Channel at 1.C; Zillow at "Location Information".

[123] KAYAK defines *personal information* as "data that identifies, relates to, describes, can be used to contact, or could reasonably be linked directly or indirectly to you"; see KAYAK at "Information We Collect and Use". The Weather Channel uses the term *personal data*, but does not define it. Zillow similarly uses the term *personal information*, but does not define it.

Throughout this paper, we document in footnotes how each privacy policy defines *personal information* and related terms. However, throughout the paper we use the term *personal information* as defined in the CCPA rather than as used in each privacy policy.

All three free apps use this personal information for both service-related and non-service-related purposes. For The Weather Channel app, service-related purposes principally consist of displaying local weather if it is allowed to access location data, and may also include hands-free audio weather alerts if it is allowed to access motion data.[124] For KAYAK and Zillow, service-related purposes principally consist of searches, including local searches if it is allowed to access location data.[125] For KAYAK, service-related purposes may also include booking travel through a third party[126] and integrating itineraries.[127]

Non-service-related purposes principally consist of advertising. Although a business may claim that advertising is service-related if the service is primarily supported through advertising, in this paper we classify a use of personal data as service-related only if we believe that a typical user would perceive the use as directly related to the desired functionality of the service.

All three free apps use location data for location-based advertising.[128] KAYAK and Zillow also use behavioral information that they directly collect for behavioral advertising.[129] All three free apps appear to collect some personal information solely for advertising purposes (e.g. interaction with advertising, gender, and "other software installed on your device"[130130]). We do not see how this personal information either supports core functionality or is used to offer elective functionality. On the flip side, some personal information is used solely for service-related purposes. For example, The Weather Channel promises

---

[124] The Weather Channel at 1.C-D.

[125] KAYAK at "Provide the Services"; Zillow at "Providing and improving our services".

[126] KAYAK at "Provide the Services".

[127] KAYAK at "Trips Services".

[128] KAYAK at "Location information"; The Weather Channel at 1.C; Zillow at "Location information".

[129] KAYAK at "Provide you more relevant advertising on and off our Services"; Zillow at "Personalizing your experience".

[130] KAYAK at "Device information".

not to use motion data for any purposes other than "to detect when you likely are in a moving vehicle".[131]

D. Sharing

As discussed in Section 2, the GDPR and the CCPA require a business to disclose the purposes for which it shares personal information with other businesses. The CCPA also requires a business to disclose the categories of personal information shared with either another business or a service provider.

All three free apps share personal information with both service providers and third parties. Following the definitions in CCPA (as discussed in Section 2 above), we classify an entity as a *service provider* if and only if its use of shared information is contractually limited to purposes specified by the business sharing the personal information, and if it may not further share the personal information with other entities.

It is common that a business outsources some tasks to a service provider. The Weather Channel shares personal information with service providers for data storage, customer service, audience research, and mapping service.[132] KAYAK shares personal information with service providers to process payments, hosting services, fraud detection, and ad response measurement.[133]

When a business uses an ad broker to place advertisements, one could envision two possibilities. First, the business could share personal information with the ad broker under a contract that restricts the ad broker's use of that personal information to the purpose of placing that ad. Alternatively, the business could allow the ad broker to not only use the shared personal information for the purpose of placing that ad, but also to use the shared information to build a user profile that the ad broker monetizes for its own services.

Both The Weather Channel and KAYAK share personal information with third parties for advertising purposes, without contractual limits on how the third party uses the information.[134] The Weather Channel shares location data, advertising identifiers, and your IP

---

[131] The Weather Channel at 1.D.

[132] The Weather Channel at 3.A.

[133] KAYAK at "Sharing to Process Payment Information" and "Sharing with Other Service Providers".

[134] KAYAK at "With other business partners"; The Weather Channel at 3.B, 3.D.

address.[135] KAYAK also shares "information about your searches, including the cities or destinations you search for, the types of accommodations you search for, your travel preferences, price range, intended travel dates, and the number of travelers in your party" and "information about your bookings and reservations for flights, hotels, car rentals, or other travel accommodations" with third parties, and appears not to restrict how this information is used by them.[136] We expect that many consumers would be surprised to learn of the extent and detail of the personal information shared by KAYAK. In contrast, Zillow states that it doesn't share personal information with third parties.[137] All three mobile apps also enable third parties to directly collect personal information from you.[138]

E. User Choice

As discussed in Section 2, the GDPR and the CCPA require some form of informed consent. Both allow a service or app's terms and conditions to specify that use of the service is conditioned on a user agreeing to the collection, use, and sharing of personal information in certain restricted situations. In particular, the CCPA allows a business to mandate in the terms and conditions of a service the *collection* and *use* of any personal information it desires, but not the *sharing* of personal information with other businesses. The GDPR only allows a business to mandate in terms and conditions collection, use, and/or sharing of personal information that is necessary for the performance of the contract between the user and the business.

The three free apps differ somewhat in the choices they afford users over the collection, use, and sharing of their personal information. Neither KAYAK nor Zillow afford users any choice over the *collection* or *use* of personal information, other than choices provided by the mobile operating system itself (e.g., whether location data may be collected and whether it may be collected only while using the app).[139]

With respect to user choices over *sharing* of personal information, in this paper we focus on choices afforded directly by the app

---

[135] The Weather Channel at 3.B.

[136] KAYAK at "Sharing with Our Business Partners".

[137] Zillow at "Sales of personal information".

[138] The Weather Channel at 3.D; Zillow at "Sales of personal information".

[139] KAYAK at "Your Choices and Rights"; Zillow at "Privacy tools and choices".

or service. We discount choices provided by the mobile operating system itself (e.g., whether advertising identifiers are active on the device), as well as options afforded through the Digital Advertising Alliances *AdChoices* icon (which, as many others have noted, are poorly understood by consumers and temporary due to their reliance on cookies).

While The Weather Channel app similarly does not afford users any choice over the *collection* of personal information, it does afford users limited control over the *use* or *sharing* of personal information; Californians may opt-out of third parties use of personal information for purposes other than advertising within the app, or a user can opt-in to a paid version of the app which eliminates in-app ads and thus presumably may eliminate sharing of personal information for advertising. KAYAK gives users who have a KAYAK account the ability to opt-out of the sharing of their personal information with third parties.[140] To satisfy CCPA requirements, KAYAK's mobile app allows Californians to opt-out of the sharing of their personal information with third parties, even if they do not have a KAYAK account. Zillow doesn't share personal information with third parties, and thus no user choices over sharing are relevant.

5. MOBILE APPS FOR PAID SERVICES (CHASE, UBER, AND UNITED)

Many services offer a mobile app that can be used in conjunction with the service. We analyze here three popular apps: Chase Mobile[141] (a banking app), Uber[142] (a ride sharing app), and United[143] (an airline app). Our goal is to compare their collection, use, and sharing of personal information with each other, to compare these practices to those of mobile apps that are primarily supported by advertising, and to compare these practices to those of other types of online services.

---

[140] KAYAK at "Your Choices and Rights".

[141] JPMorganChaseBank,"OnlinePrivacyPolicy"(Chase), Jan. 15, 2020, https://www.chase.com/digital/resources/privacy-security/privacy/online-privacy-policy.

[142] Uber Technologies Inc.,"UberPrivacyNotice"(Uber), Oct. 27, 2020, https://www.uber.com/legal/en/document/?name=privacy-notice&country=united-states&lang=en.

[143] United Airlines Inc.,"CustomerDataPrivacyPolicy"(United), Jan. 15, 2016, https://www.united.com/ual/en/us/fly/privacy.html.

A. Scope

Each of the three privacy policies apply to the service's mobile apps and websites.[144] Some policies also apply to other services (e.g., United Airlines offline customer service).[145] We focus here only on the mobile apps.

Some mobile apps are owned by parent companies that operate other services. JPMorgan Chase Bank is owned by a parent company whose subsidiaries include other financial businesses, and JPMorgan Chase Bank both collects personal information from and shares personal information with these other subsidiaries.[146]

B. Collection

Since these paid apps are only useful to users who have accounts with the associated services and are logged into their account through the app, all three companies already have contact information (e.g., name, address, email address, phone number), whereas some of the free mobile apps do not.[147] All three paid apps collect similar device identifiers (e.g., IP address and other unspecified device identifiers) as do the free apps.[148] However, whereas the free apps also collect advertising identifiers (e.g., Apple or Android advertising identifier), it is unclear whether all of these paid apps do.[149]

The paid apps collect similar types of *behavioral information* as do the free apps. This includes devices used by a consumer (e.g., "the hardware models, ..., operating systems and versions, [and]

---

[144] Chase; Uber at II.A; United at "Scope of this policy".

[145] United at "Scope of this policy".

[146] Chase at "Disclosure of Information" and "Online advertising".

[147] Chase at "Personal Information"; Uber at III.A.1; United at "Information we collect about you".

[148] Chase at "Usage and Other Information" and "Chase Mobile"; Uber at III.A.2 "Device data"; United at "Information we collect automatically" and "Information we collect through our mobile application(s)".

[149] Uber collects advertising identifiers; see Uber at III.A.2 "Device data". Chase collects "device identifiers", but it is unclear whether these identifiers include advertising identifiers; see Chase at "Chase Mobile". United might not collect advertising identifiers, since it only collects the "[d]evice ID or alternative ID where required by the platform provider"; see United at "Information we collect through our mobile application(s)".

software"[150]) and app usage (e.g., "[f]eatures you use and links you click" and "[a]mount of time spent in the application"[151]). The paid apps also collect similar information on user interests as do many free apps. For example, both Uber and United collect information about trip destinations, similar to the information that KAYAK collects.[152]

The paid apps also collect similar information as do the free apps about a user's location, using information provided by mobile devices (e.g., IP address, accessible Wi-Fi networks, accessible cell towers, and GPS information).[153] Uber may also collect "device motion data", similar to The Weather Channel.[154] As with free apps, location data may be either collected only while using the app or at all times, depending on the privacy setting selected by the user within the mobile operating system.[155] However, whereas the free apps typically collect location data at all times, if allowed by the privacy setting, some paid apps choose to track a user's location only at limited times and places. For example, United tracks location continuously only "while at or near certain airports in the U.S.".[156]

These three paid apps are in a partially privileged position to observe the behavioral information that they collect. All of the associated services have substantial competition, but once a consumer chooses a particular service, there are often no competing mobile apps that work with that chosen service.

C. Use

All three paid apps use this personal information[157] for both service-related and non-service-related purposes. However, for the

---

[150] Uber at III.A.2 "Device data".

[151] United at "Information we collect through our mobile application(s)".

[152] Uber at III.A.2 "Location data (riders and delivery recipients)"; United at "Use of cookies, web beacons and other similar technologies".

[153] Chase at "Usage and Other Information" and "Chase Mobile"; Uber at III.A.2 "Location data (riders and delivery recipients)"; United at "Information we collect automatically" and "Information we collect through our mobile application(s)".

[154] Uber at III.A.2 "Device data".

[155] KAYAK at "Location information"; The Weather Channel at 1.C; Zillow at "Location Information".

[156] United at "Information we collect through our mobile application(s)".

[157] None of these three paid apps define *personal information* or related terms. Chase uses the term *personal information* to describe contact information, but excludes

paid apps the service-related purposes dominate. The Chase app uses your contact information and financial information to check account balances, pay bills, and deposit checks; and it uses your location (if permitted) to find local ATMs. The Uber app uses your location to determine your pickup location (if permitted) and to track your ride.[158] The Uber app also uses behavioral information to match riders with drivers (e.g., "we prevent matches if one has given the other a one-star rating in the past").[159] The United app uses your contact information to book flights and check-in for flights, and uses your location in airports for location-based maps.[160]

That said, all three paid apps also use personal information for advertising. All use behavioral information, including location, both for their own advertisements and for advertisements of third parties.[161] Given the sensitivity of much of the personal information collected by paid apps, we expected their privacy policies to promise that sensitive information would not be used for advertising; however, we found no such disclosures in these privacy policies. Indeed, United may use "data collected about you … through your use of our mobile apps" for targeted advertising by third parties.[162]

D. Sharing

Similar to the free apps, all three paid apps share personal information with both service providers and third parties. The purposes for sharing personal information with service providers are similar to those of free apps, including anti-fraud services, auditing services, payment providers, cloud storage, and data analytics.[163]

"usage and other information"; see Chase at "Information we collect". In contrast, Uber uses the term *personal data* to describe both contact information and usage data; see Uber at III.F.a.

[158] Uber at III.A.2 "Location data (riders and delivery recipients)".

[159] Uber Technologies Inc.,"Matching", undated, accessed Nov. 16, 2020, https://marketplace.uber.com/matching.

[160] United at "Information collected from our mobile application(s)".

[161] Chase at "Online advertising"; Uber at III.B.6; United at "Information collected from our mobile application(s)".

[162] United at "Targeted advertising".

[163] JPMorgan Chase Bank, "California Consumer Privacy Act (CCPA) Disclosure" (Chase California), January 1, 2020, https://www.chase.com/digital/resources/privacy-security/privacy/ca-consumer-privacy-act, at "Categories of Third Parties to

Given that paid apps are presumably primarily intended as companions to a paid service, we expected their privacy policies to severely limit sharing of personal information with third parties. However, their privacy policies are often anything but clear about such limits. United shares personal information with third parties such as airlines, car rental agencies, hotels and travel agencies "for their own marketing purposes".[164] Uber shares personal information with "[m]arketing partners and marketing platform providers" and with "[r]estaurant partners".[165] However, both United and Uber fail to disclose any limits on what personal information is shared. In its nationwide privacy policy, Chase discloses that it may share personal information with third parties "to bring you co-branded services, products or programs", but the privacy policy similarly fails to disclose any limits on what types of products or programs are included or on what personal information is shared.[166] Even more confusing, Chase's California privacy policy does *not* disclose any sharing for advertising by third parties.[167] Thus, while the personal information shared by paid apps for third party advertising *might* be more limited than the detailed personal information shared by free apps such as KAYAK, this is anything but clear.

E. User Choice

We similarly expected that the privacy policies of paid apps would afford users more choices over the collection, use, and sharing of personal information than those of free apps. However, the differences between various paid apps and various free apps are larger than the differences between free and paid apps as a whole. None of these three paid apps afford users any choice over the *collection* and *use* of personal information, other than choices provided by the mobile operating system itself (e.g., whether location data may be collected and whether it may be collected only while using the app, and whether advertising identifiers are active on the device).

Whom Personal Information is Disclosed"; Uber at III.D.6; United at "Disclosing your information".

[164] United at "Marketing partners".

[165] Uber at III.D.6.

[166] Chase at "Disclosure of Information".

[167] Chase California at "Categories of Third Parties to Whom Personal Information is Disclosed".

With respect to *sharing* of personal information, Uber states that it "does not sell or share user personal data with third parties for their direct marketing, except with users' consent".[168] However, Uber recognizes that, under the CCPA, "some sharing of personal information necessary to provide you with personalized ads may be considered a 'sale,' even if no money is exchanged", and thus gives Californians the choice to opt-out of Uber "sharing your information with some of its advertising partners".[169] United allows users to opt-out of "receiving marketing or promotion-related emails or direct mail from United".[170] However, it is unclear whether users can opt-out of United sharing of personal information with third parties, and United's homepage does not include the CCPA's required option for Californians to opt-out of such sharing. Chase does not afford uses any choices over the sharing of personal information for advertising. Apparently, Chase believes it is exempt from the user choice requirements in CCPA, stating that "[w]hile we often benefit from [sharing of personal information with third parties], we do not share personal information for the sole purpose of receiving compensation for that information"[171]

6. APPLICATION SUITES (GOOGLE, MICROSOFT, AND APPLE)

A relatively small number of companies offer widely used application suites of consumer services that integrate personal information collected through each product within the application suite. We consider Google, Microsoft, and Apple.

A. Scope

Google, Microsoft, and Apple each has a single privacy policy that applies to most of its application suite. Google's privacy policy applies to most of its consumer services, including Google Search, Gmail, Google Drive, the Chrome browser, the Android operating system, Google Maps, Google Home, Google Play Store, and

---

[168] Uber at III.B.

[169] Uber Technologies Inc., "For California Consumers" (Uber California), undated, accessed November 16, 2020, https://privacy.uber.com/privacy/california.

[170] United at "Opting out".

[171] Chase California at "Sale of Personal Information".

YouTube.[172] Some Google services, including the Chrome browser, have separate privacy policies that substitute for or supplement Google's main privacy policy.[173] Microsoft's privacy policy applies to most of its consumer services, including Microsoft Office, Windows, Skype, LinkedIn, Xbox, OneDrive, Outlook, the Edge browser, Bing, and the Microsoft Store.[174] However, many Microsoft services have separate privacy policies that substitute for or supplement Microsoft's main privacy policy. Apple's privacy policy applies to most of its consumer services, including Apple devices (e.g., Mac, iPad, and iPhone), Apple App Store, Apple TV+, Apple Music, Apple News+, the Safari browser, and iCloud.[175]

Google collects personal information not only directly through its own consumer services, but also indirectly from consumers through third parties that use Google's advertising platform. Google's privacy policy does not apply to collection of personal information from third parties. Instead, Google has a separate disclosure about such collection and use of personal information from third parties[176], and Google requires that third parties using its advertising platform include specific disclosures about Google collection and use of personal information[177]. Unlike Google, Microsoft does not have its own advertising platform which can be used to collect personal information indirectly from consumers through third parties. Similar to other businesses, however, Microsoft does obtain personal information from third parties, including "[d]ata brokers from which we purchase demographic data", "[s]ervice providers that help us determine your device's location", and "[p]artners with which we offer co-branded services or engage in joint marketing activities".[178]

---

[172] Google, "Google Privacy Policy" (Google), September 30, 2020, https://policies.google.com/privacy?hl=en-US, at "Introduction".

[173] Google at "Specific Google Services".

[174] Microsoft, "Microsoft Privacy Statement" (Microsoft), November, 2020, https://privacy.microsoft.com/en-us/privacystatement.

[175] Apple, "Privacy Policy" (Apple), December 31, 2019, https://www.apple.com/legal/privacy/en-ww/.

[176] Google,"Advertising"(GoogleAdvertising),undated,accessedNovember16,2020, https://policies.google.com/technologies/ads.

[177] Google, "AdSense Program Polices Required Content" (Google AdSense), undated, accessed November 16, 2020, https://support.google.com/adsense/answer/1348695?hl=en.

[178] Microsoft at "Personal data we collect".

B. Collection

Similar to the mobile apps discussed above, Google, Microsoft, and Apple each collect a wide range of personal identifiers, including device identifiers (e.g., IP address and IMEI), and advertising identifiers (e.g., Apple or Android advertising identifier).[179] Google, Microsoft, and Apple also create and collect their own personal identifiers. Google creates cookies that can "uniquely identify a browser, app, or device"[180]; Microsoft creates the Windows advertising identifier, "a unique advertising ID for each person using a device" that is running the Windows operating system[181]; and Apple creates the Apple advertising identifier and the Apple ID identifier. However, Google has the ability to collect its own personal identifiers across a dramatically larger percentage of websites than does Microsoft or Apple. Whereas some mobile apps operate without a login and some only operate when logged in, the application suites offered by Google, Microsoft, and Apple often can operate in either mode. Consequently, Google, Microsoft, and Apple often collect contact information (e.g., name, address, email address, and phone number).[182]

The application suites collect a far more extensive range of behavioral information than do mobile apps, based on their technical ability and the nature of each of their services.

Some of the behavioral information focusses on a user's usage of the apps provided by the business, as do the mobile apps. Google collects "the date, time, and referrer URL ... when a Google service on your device contacts our servers"[183]; Microsoft collects the "features you use" of Microsoft products[184]; and Apple collects "how you use your device and applications"[185]. However, because the application suites receive far more use than do individual mobile apps, they

---

[179] Google at "Unique identifiers"; Microsoft at "Personal data we collect"; Apple at "What personal information we collect" and at "Cookies and Other Technologies".

[180] Google at "Unique identifiers".

[181] Microsoft at "Advertising ID".

[182] See e.g. Google at "We want you to understand the types of information we collect as you use our services", in the pop-up window for "personal information".

[183] Google at "Your apps, browsers & devices".

[184] Microsoft at "Personal data we collect".

[185] Apple at "Collection and Use of Non-Personal Information".

correspondingly collect more information about a user's usage of these apps.

Other behavioral information focusses on devices used by a consumer and on apps offered by other businesses that a user utilizes. Google collects "the apps, browsers, and devices you use to access Google services" and apps installed from the Google Play Store[186]; Microsoft collects "[d]ata about your device and the product ... you use" of Microsoft products and devices running Windows[187] and "how you access and use Microsoft Store; the products you've viewed, purchased, or installed"[188]; and Apple collects information about Apple devices and apps downloaded through the Apple App Store[189]. While mobile apps also often collect information about the apps and devices used by a consumer, because the providers of the application suites operate app stores, they have far greater knowledge of the full range of applications that a user installs on their devices.

Yet other behavioral information focusses on user interests. Google collects "[t]erms you search for, [v]ideos you watch, [v]iews and interactions with content and ads, ..., [p]urchase activity, ..., [a]ctivity on third-party sites and apps, ..., and Chrome browsing history you've synced with your Google Account"[190], and user interactions with ads (including "how you move your mouse over an ad")[191]. Microsoft collects "the webpages you visit", "your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic", "media content (e.g., TV, video, music, audio, text books, apps, and games) you access through our products", and "[s]earch queries and commands when you use Microsoft products with search or related productivity functionality".[192] Apple collects "browsing activity", "usage of Apple Books", "[y]our purchase information" using Apple ID, "usage of Apple Music", "usage of Apple TV", and Safari "search queries, the Safari Suggestions you select, and

---

[186] Google at "Your apps, browsers & devices".

[187] Microsoft at "Personal data we collect".

[188] Microsoft at "Microsoft Store".

[189] Apple at "Collection and Use of Non-Personal Information".

[190] Google at "Your activity".

[191] Google at "Your activity" in the pop-up widow for "Views and interactions with content and ads".

[192] Microsoft at "Personal data we collect".

usage data".[193] Whereas mobile apps also often collect behavioral information about user interests, the application suites have access to a far broader and richer set of such personal information.

Similar to many mobile apps, the application suites by Google, Microsoft, and Apple also collect information about a user's location when using their services, using information provided by mobile devices (e.g., accessible Wi-Fi and Bluetooth networks, accessible cell towers, GPS information, and sensor data).[194]

The application suites are much more likely than mobile apps to support a user's creation of substantial amounts of personal information. For Google services which support the creation of personal information (e.g., Gmail, Google Drive, YouTube), Google collects content created by users.[195] Apple similarly collects content created using Apple products (e.g., iCloud).[196] Microsoft similarly collects content created using Microsoft products (e.g., Office, OneDrive, Outlook).[197] For example, "if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user" and "[i]f you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox".[198] It is critical, however, to note that Microsoft does not collect the content of files unless you place them in OneDrive or use optional features such as Translator.[199]

The application suites differ on collection of audio. For Google services which include audio features, Google collects "[v]oice and audio information".[200] Similarly, for Microsoft services which include audio features (e.g., Cortana), Microsoft collects "[y]our voice data, such as the search queries or commands you speak, which may include

---

[193] Apple, "California Privacy Disclosures" (Apple California), February 26, 2020, https://support.apple.com/en-us/HT210807.

[194] Google at "Your location information"; Microsoft at "Personal data we collect"; Apple at "Location-Based Services".

[195] Google at "Things you create or provide to us".

[196] Apple at "What personal information we collect" and "Collection and Use of Non-Personal Information".

[197] Microsoft at "Personal data we collect".

[198] Microsoft at "Personal data we collect".

[199] Microsoft at "Microsoft 365".

[200] Google at "Your activity".

background sounds".[201] In contrast, Apple does not generally collect audio information.[202]

The application suites also collect information about people with whom you communicate using their services. Google collects the identities of "[p]eople with whom you communicate or share content".[203] Microsoft collects "your contacts and relationships if you use a product [e.g., Skype] to share information with others, manage contacts, communicate with others, or improve your productivity".[204] Apple similarly collects information about people with whom you communicate using an Apple service.[205]

As discussed in Section 2, both the GDPR and the CCPA require a business to disclose, at a minimum, the categories of sources of personal information. All three companies obtain some personal information from third parties, e.g. "third party developers may provide us with information about your activity in their apps".[206] However, Google also collects personal information *indirectly* from consumers through third parties that use Google's advertising platform.[207] This personal information includes personal identifiers (principally, cookies) and behavioral information (principally, app usage and user interests).[208] Microsoft and Apple do not have similar extensive advertising platforms.

The application suites are in a substantially more privileged position than are the mobile apps to observe much of the behavioral information that they collect. Some of this privilege derives from the breadth of their application suites. Other privilege derives from the popularity of some of their consumer services. Google's suite includes

---

[201] Microsoft at "Personal data we collect". Translator does not log any portion of the translation request.

[202] Apple California. See also Apple, "Privacy" (Apple Privacy), undated, accessed Apr. 1, 2020, https://www.apple.com/privacy/.

[203] Google at "Your activity".

[204] Microsoft at "Personal data we collect".

[205] Apple at "What personal information we collect" and "Collection and Use of Non-Personal Information".

[206] Apple California.

[207] Google Advertising at "Our advertising cookies". Google's advertising platform includes "AdSense, AdWords, Google Analytics, and a range of DoubleClick-branded services".

[208] Google, "Types of Cookies Used by Google" (Google Cookies), undated, accessed November 16, 2020, https://policies.google.com/technologies/types.

Google Search, the Chrome browser, the Android operating system, and YouTube, all of which have large market shares. Since Microsoft's consumer product suite overlaps considerably with Google's, the behavioral information is similar in type. However, since they have very different market shares in each product, the behavioral information of each type collected likely differs substantially in volume.

Google's privilege also derives in part from the popularity among third parties of Google's advertising platform. With respect to behavioral information focusing on user interests, Google and Microsoft have different views and somewhat different interests. Google has the ability to collect user interests across a wide range of websites, whereas Microsoft has the ability to collect user interests on devices running Windows. Google, however, has a much stronger interest in collecting personal information about user interactions with ads.

C. Use

All three companies uses this personal information[209] for both service-related and non-service-related purposes.[210]

Service-related purposes are manifold. Many services within each application suite require some personal information to provide basic functionality. Google Search and Bing use your search terms to provide search results. Gmail, Outlook, and the Apple Mail app use the identities of people with whom you communicate to deliver email. Google Drive, OneDrive, and iCloud store content created by you in

---

[209] Google defines *personal information* as "information that you provide to us which personally identifies you, such as your name, email address, or billing information, or other data that can be reasonably linked to such information by Google, such as information we associate with your Google Account."; see Google at "We want you to understand the types of information we collect as you use our services" in the pop-up window for "personal information". Microsoft uses the term *personal data*, but does not define it. Apple defines *personal information* as "data that can be used to identify or contact a single person"; see Apple at "Collection and Use of Personal Information". Apple refers to *non-personal information* as "data in a form that does not, on its own, permit direct association with any specific individual"; see Apple at "Collection and Use of Non-Personal Information". Apple states that "[i]f we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined."; see Apple at "Collection and Use of Non-Personal Information".

[210] Google at "Why Google collects data".

the cloud. The Chrome, Edge, and Safari browsers store bookmarked websites. Google Home, Cortana, and Siri listen to a user's audio commands.

Some application suite services offer additional functionality if they are able to use additional personal information. Google Maps can offer turn-by-turn directions if it is allowed to access a user's location. Gmail, Outlook, and Apple Mail apps may place event information into Google Calendar, Outlook calendar, and Apple's calendar app (respectively) if they are allowed to access the content of email. Office may offer collaborative editing it is able to store the document on OneDrive.[211] Skype may use contact information if it is allowed to access your Outlook contact list.[212]

However, the design of each application suite affects the amount of personal information used in many of these services. Apple restricts use of personal information[213] much more severely than either does Google or Microsoft. Indeed, Apple is marketing its services in part based on its privacy practices. Much of the behavioral information that Apple collects is not associated with persistent personal identifiers. For example, any information that Apple collects through Apple Maps, Siri, or Apple News "is not associated with your identity"[214], and search queries are not "associated with your IP address"[215].

Non-service-related purposes for each company principally consist of advertising. However, the extent and reach of their advertising businesses are very different. For Google, advertising is its principal business, and most of its application suite is often free to consumers. Consequently, Google uses much of the personal information it

---

[211] Microsoft at "Microsoft 365".

[212] Microsoft at "Skype".

[213] Apple defines *personal information* as "data that can be used to identify or contact a single person"; see Apple at "Collection and Use of Personal Information". Apple refers to *non-personal information* as "data in a form that does not, on its own, permit direct association with any specific individual"; see Apple at "Collection and Use of Non- Personal Information". Apple states that "[i]f we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined."; see Apple at "Collection and Use of Non-Personal Information". However, in this paper we use the term *personal information* as defined in the CCPA.

[214] Apple California.

[215] Apple at "Collection and Use of Non-Personal Information".

collects to "show you personalized ads based on your interests".[216] It also combines personal information it collects from different services.[217] For Microsoft, its product suite generates a considerable amount of income, and advertising is a side business. Consequently, although Microsoft uses some types of personal information for behavioral advertising both in Microsoft's own products and on third-party sites (e.g. "we may predict your interest in gaming and communicate with you about new games you may like"[218]), it generates far less revenue from advertising on third-party sites than does Google. For Apple, its hardware generates a considerable amount of income, and its application suite helps sell the hardware; advertising is principally for Apple's own products. Consequently, Apple uses some types of personal information (e.g. devices and content downloads) to create audience segments for behavioral advertising in Apple's own products (e.g., Apple News and Apple App Store).[219]

As with the mobile apps, it is often difficult to determine which types of personal information are used for advertising. However, each of the application suites discloses some types of personal information that are *not* so used. For example, Google does not use private documents stored on Google Drive for advertising[220], and it does not "scan or read your Gmail messages to show you ads" [221]. Similarly, Microsoft "does not use what you say in email, chat, video calls, or voice mail, or your documents, photos, or other personal files to target ads to you".[222]

D. Sharing

Google, Microsoft, and Apple each share personal information with both service providers and third parties.[223]

---

[216] Google at "Provide personalized services, including content and ads".

[217] Google at "Protect Google, our users, and the public".

[218] Microsoft at "How we use personal data".

[219] Apple at "Cookies and Other Technologies" and Apple California.

[220] Google, "Google Drive Terms of Service" (Google Drive), undated, accessed November 16, 2020, https://support.google.com/drive/answer/2450387?hl=en.

[221] Google,"HowGmailadswork"(GoogleGmail),undated,accessedNovember16, 2020, https://support.google.com/mail/answer/6603?hl=en.

[222] Microsoft at "How we use personal data".

[223] Google at "Sharing your information"; Microsoft at "Reasons we share personal data"; Apple California.

Sharing with service providers is similar among the three companies. The purposes for which Microsoft shares personal information with service providers includes "customer service support" and "protecting and securing our systems and services".[224] The purposes for which Google shares personal information with service providers includes unspecified types of processing.[225]

All share personal information at a user's direction and with user consent for optional functionality (e.g. "when you send an email to a friend" or "share photos and documents on OneDrive" [226], and sharing of contact information with a booking service to make a reservation[227]).

However, beyond such user-directed sharing, sharing with third parties is very different among the three companies. Microsoft shares some personal information with third parties for advertising.[228] Such personal information appears to be the combination of a personal identifier (e.g., IP address and Windows advertising identifier) with audience segments (e.g., based on "your interests and favorites, your location, your transactions, how you use our products, your search queries, or the content you view").[229] Apple restricts sharing of personal information more than does Microsoft. By default, Apple only shares the Apple Advertising Identifier with third parties. Apple does not share other personal information with third parties, except when requested by the user. [230] Google's sharing of personal information with third parties is similarly limited. Google only shares personal information[231] for legal purposes. Google may have limited need or interest in sharing personal information with third parties, since Google's advertising platform does not require such sharing in order for advertisers to place ads based on audience segments.

---

[224] Microsoft at "Reasons we share personal data".

[225] Google at "For external processing".

[226] See e.g. Microsoft at "Reasons we share personal data".

[227] Google at "With your consent".

[228] Microsoft at "Advertising".

[229] Microsoft at "Advertising".

[230] Apple California.

[231] Google also shares personal information which Google classifies as *non-personally identifiable information* with third parties; however, Google does not disclose enough information for us to determine whether such information would be classified under the CCPA as *personal information*, *de-identified information*, or *aggregate consumer information*.

E. User Choice

All three companies affords users much more extensive choices than do the mobile apps over the collection, use, and/or sharing of personal information. We discuss control over *collection, use,* and *sharing* each in turn.

With respect to *collection* of personal information, we initially expected that those companies that collected *less* data would give users *more* choices over collection of personal information. This is wrong. Google, which has the most *extensive* collection of personal information, also affords users the *most extensive* choices over its collection practices. A user can opt-out of Google's collection of much of the behavioral information it collects, including "your activity on Google sites and apps", "your searches", your location history, "the YouTube videos you watch", your contact list, "your voice and audio recordings", information about "installed apps', autofill information, and Chrome bookmarks.[232] Microsoft, which has a more *moderate* collection of personal information, affords users *some* choices, but fewer than does Google. Using Windows privacy settings, a user can opt-out of the collection of app usage data, voice data (e.g., through Cortana), "typing history and handwriting patterns", and your location. And Apple, which has the *least* collection of personal information, affords users *no* choices over this collection.

With respect to *use* of personal information, the situation flips, with Microsoft offering the most choice. Microsoft affords users *extensive* choice over the use of personal information. Many of the settings, however, are by default permissive. Using the Microsoft privacy dashboard[233], a user can opt-out the use for behavioral advertising of "your searches and other online activity associated with your Microsoft account... [or] associated with this browser". Using Windows privacy settings[234], a user can opt-out of use of the Windows advertising identifier for behavioral advertising, app usage data for

---

[232] Google Account, undated, accessed March 30, 2020, https://myaccount.google.com/.

[233] Microsoft privacy dashboard, https://account.microsoft.com/privacy/.

[234] Microsoft Windows 10 privacy settings, available at Settings -> Privacy.

personalized recommendations and behavioral advertising, "activity history"[235] for personalization, cloud-based speech recognition, and inking & typing personalization. Using settings in the Edge browser[236], a user can opt-out of the use of Edge browsing history for behavioral advertising. Some of the settings are by default restrictive. Using settings in the Edge browser, a user can opt-in to synchronization of bookmarks with other devices. In contrast, Apple affords users only a *single* choice of the use of personal information for behavioral advertising by Apple.[237] This same choice, called *Limit Ad Tracking*, simultaneously stops sharing of the Apple Advertising Identifier with third parties.[238] Google is even more limited. A user can opt-out of the use of personal information for ad personalization on Google services (e.g., Search, YouTube). However, a user cannot opt-out of the use of personal information for ad personalization on non-Google services that use the Google advertising platform.

With respect to *sharing* of personal information, the situation is again different, with Apple offering the most choice. Apple affords users *granular* choices over the sharing of personal information with third parties, e.g., through separate privacy settings for each app for sharing of contacts, calendars, location, and photos. Microsoft affords users similar choices. Using Windows privacy settings, a user can opt-in to the sharing of location, camera, microphone, contacts, calendar, email, tasks, pictures, videos, documents libraries, and OneDrive files with a variety of apps. Google is different. Since Google primarily shares personal information only at a user's direction and with user consent for optional functionality, this consent simultaneously affords users controls over which personal information is shared with which third parties for purposes other than advertising.

7. SOCIAL NETWORKS (FACEBOOK, TWITTER, AND PINTEREST)

Facebook has the dominate market share for social networks. We analyze its privacy policy here.

---

[235] *Activity history* "helps keep track of the things you do on your device, such as the apps and services you use, the files you open, and the websites you browse". See Microsoft at "Activity history".

[236] Microsoft Edge Privacy and services settings, edge://settings/privacy.

[237] Apple at "Cookies and Other Technologies".

[238] Apple at "Cookies and Other Technologies".

A. Scope

Facebook has a single privacy policy that applies to Facebook, Instagram, Messenger, and other Facebook products[239], Twitter has a single privacy policy that applies to Twitter and the Periscope mobile app[240], and Pinterest has a single privacy policy that applies to its service[241]. Each of these policies covers both the web versions and the mobile apps.

Like Google, Facebook collects personal information not only directly through its own consumer services, but also indirectly from consumers through third parties that use Facebook's advertising platform. However, it is unclear whether Facebook's privacy policy applies to collection of personal information from third parties. It is discussed in the privacy policy, but supplemented by disclosures regarding Facebook and Instagram cookies on third party sites.[242] Like Google, Facebook requires that third parties using its advertising platform include specific disclosures about Facebook collection and use of personal information[243].

Although Twitter and Pinterest collect personal information from third parties, as do many of the service and application providers discussed in this paper, they do not operate an advertising platform outside their own services.

B. Collection

Similar to all of the cases discussed above, Facebook, Twitter, and Pinterest each collect a wide range of personal identifiers,

---

[239] Facebook, "Data Policy" (Facebook), August 21, 2020, https://www.facebook.com/policy.php.

[240] Twitter, "Twitter Privacy Policy" (Twitter), June 18, 2020, https://www.twitter.com/en/privacy.

[241] Pinterest, "Privacy Policy" (Pinterest), September 2, 2020, https://policy.pinterest.com/en/privacy-policy.

[242] Facebook at "Information from partners".

[243] Facebook,"FacebookBusinessToolsTerms"(FacebookBusiness),December26, 2019, https://www.facebook.com/legal/technology_terms.

including device identifiers (largely unspecified), and advertising identifiers (unspecified).[244]

Like Google, Microsoft, and Apple, all three companies (Facebook, Twitter, and Pinterest) also create and collect their own personal identifiers using cookies. These personal identifiers allow Facebook to combine information "across different devices you use"[245], and similarly allows Twitter to "infer that certain devices are associated with one another"[246]. In addition, Twitter associates different email addresses that share the same last name to create an inferred identity.[247] Facebook has the ability to collect its own personal identifiers across a larger percentage of websites than does Microsoft or Apple, but less than does Google.

Unlike Google, Microsoft, and Apple, all three companies (Facebook, Twitter, and Pinterest)'s's services are principally used while logged in, and thus they almost always collects contact information that you provide when you sign up for an account.[248]

Facebook, Twitter, and Pinterest collect a far more extensive range of behavioral information than do mobile apps, based on the nature of their services.

Some of the behavioral information each collects focusses on usage of its apps, as do the mobile apps and the application suites. Facebook collects "information about how you use our Products, such as ... the features you use; the actions you take; ... and the time, frequency and duration of your activities."[249] Twitter collects log data that includes "when you install another application through Twitter".[250] Pinterest collects log data that include "[a]ctions taken during [a]

---

[244] Facebook at "Identifiers"; Twitter at "You should read this policy in full, but here are a few key things we hope you take away from it" and at "Log Data"; Pinterest at "We also get technical information when you use Pinterest". We could not determine whether Pinterest collects advertising identifiers.

[245] Facebook at "Device Information".

[246] Twitter, "Our use of cookies and similar technologies" (Twitter Cookies), undated, accessed October 20, 2020, https://help.twitter.com/en/rules-and-policies/twitter-cookies#, at "Personalized content".

[247] Twitter at "Personalizing Based on Your Inferred Identity".

[248] Facebook at "Things you and others do and provide"; Twitter at "Basic Account Information", and Pinterest at "When you give it to us or give us permission to obtain it".

[249] Facebook at "Your usage".

[250] Twitter at "Log Data".

session".[251] However, because the application suites receive far more use than do these social network services, they collect more information about app usage.

Other behavioral information focusses on devices used by a consumer and on apps offered by other businesses that a user utilizes, as do others. Facebook collects "information from and about the computers, phones, connected TVs and other web-connected devices you use that integrate with our Products" as well as "information about other devices that are nearby or on your network", including "the operating system, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins" and "information about operations and behaviors performed on the device, such as whether a window is foregrounded or backgrounded, or mouse movements".[252] This list of information that Facebook collects about apps other than Facebook, and about devices that aren't being used to access Facebook, is astounding. Neither Twitter nor Pinterest collect similar information. Facebook might have less technical ability to collect information about other apps on consumer devices than do providers of operating systems (e.g., Microsoft and Apple), but Facebook is clearly aggressive in collecting whatever device and app information it has the technical ability to collect.

Yet other behavioral information focusses on user interests. Facebook collects "the types of content you view"[253], Twitter collects "information when you view content on or otherwise interact with our services" including "search terms"[254], and Pinterest collects "which Pins you click on"[255]. Whereas Google has superior information about user searches, Facebook, Twitter, and Pinterest still have considerable insight into content viewed.

Similar to many mobile apps and the application suites, all three social networks collect information about a user's location when using their services, using information provided by mobile devices (e.g., accessible Wi-Fi and Bluetooth networks, accessible cell towers,

---

[251] Pinterest, "Technical Information We Collect When You Use Our Service" (Pinterest Technical Information), undated, accessed October 20, 2020, https://policy.pinterest.com/en/technical-information-we-collect-when-you-use- our-service.

[252] Facebook at "Device Information".

[253] Facebook at "Your usage".

[254] Twitter at "Log Data".

[255] Pinterest at "Clickstream data and inferences".

and GPS information).[256] But Facebook also collects "information in or about the content you provide (like metadata), such as the location of a photo"[257], and Pinterest similarly collects "geo-location data, when shared through … photos"[258].

Like the application suites, social networks are much more likely than mobile apps to support a user's creation of substantial amounts of personal information. Facebook collects "the content, communications and other information you provide when you use our Products".[259] Twitter collects "your Tweets", "Periscope broadcasts you create", and "content you contribute to another account's broadcast".[260] Pinterest collects "boards you create, and any text that you add in a comment or description".[261] Unlike Microsoft, which does not collect the content of files unless you are place them in OneDrive or use optional features such as Office Translator, these social networks collect all such content.

Facebook, but not Twitter or Pinterest, also collects audio, images, and video, including "what you see through features we provide, such as our camera".[262] This collected media may parallel or exceed that collected by Google and by Microsoft. In contrast, Apple does not generally collect audio information.

Not surprisingly, all three social networks collect information about people with whom you communicate using its services. Facebook collects "information about the people, Pages, accounts, hashtags and groups you are connected to and how you interact with them across our Products"[263] , and Twitter collects "information about whom you have communicated with and when"[264]. All three also collect the content of communications. Facebook collects the content of communications when you "message or communicate with others"[265], and Twitter

---

[256] Facebook at "Device signals", "Data from device settings", and "Network and connections"; Twitter at "Location Information", and Pinterest at "We collect information in a few different ways".

[257] Facebook at "Things you and others do and provide".

[258] Pinterest at "California residents".

[259] Facebook at "Things you and others do and provide".

[260] Twitter at "Public Information".

[261] Pinterest at "Clickstream data and inferences".

[262] Facebook at "Things you and others do and provide".

[263] Facebook at "Networks and connections".

[264] Twitter at "Direct Messages and Non-Public Communications".

[265] Facebook at "Information and content you provide".

"store[s] and process[es] your communications"[266]. This information is likely to exceed similar information collected by Google, Microsoft, or Apple; whereas Google, Microsoft, and Apple collect information about people with whom you communicate, they do not collect the same scope of content of communications.

Finally, like Google, Facebook also collects personal information indirectly from consumers through third parties that use Facebook's advertising platform.[267] Although Twitter does not operate a similar advertising platform, it also collects personal information indirectly from consumers through third parties that use incorporate Twitter icons and cookies.[268] This personal information includes personal identifiers (principally, cookies) and behavioral information (principally, app usage and user interests).[269]

Comparisons between the collection abilities of social networks and of the application suite providers are difficult. The application suites have a greater breadth in their products than do the social networks. Google has a large market share in search. Google and Facebook both have strong capabilities to collect behavioral information through their advertising networks. However, Facebook and Twitter collect very detailed information about users interests from those using their services.

C. Use

As with other companies, social networks use this personal information[270] for both service-related and non- service-related purposes.

---

[266] Twitter at "Direct Messages and Non-Public Communications".

[267] Facebook at "Information from partners". Facebook's advertising platform includes "social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, [and] the Facebook pixel."

[268] Twitter Cookies at "Where are these technologies used?".

[269] Facebook, "Cookies & Other Storage Technologies" (Facebook Cookies), October 5, 2020, https://www.facebook.com/policies/cookies/', Twitter Cookies at "Personalization across devices".

[270] In its nationwide privacy policy, Facebook uses the term *information* rather than *personal information*. It characterizes "information that personally identifies you" as "information such as your name or email address that by itself can be used to contact you or identifies who you are"; see Facebook at "Advertisers". In contrast, in its California privacy policy, Facebook uses the term *personal information*, and adopts

Service-related purposes center around constructing the view each user is presented of their social network and its activity. Facebook uses device information to "help you stream a video from your phone to your TV."[271] It uses the content you provide to populate your friends' News Feed.[272] It uses the content you have viewed to personalize your News Feed and to "make suggestions for you (such as groups or events you may be interested in or topics you may want to follow)".[273] It uses information about connections between people to "suggest that you join a group on Facebook that includes people you follow on Instagram or communicate with using Messenger".[274] It uses photos for face recognition.[275] Similarly, Pinterest uses personal information about users interests to "[r]ecommend Pins, boards, topics or categories you might like based on your activity on Pinterest", uses location to show you a local retailer's Pins, and uses photos to show you similar items.[276] Twitter uses location "to operate or personalize our services including with more relevant content like local trends, stories, ads, and suggestions for people to follow".[277]

While this is in some respects similar to the use of information by Google or Microsoft to enable functionalities in their products, Facebook doesn't attempt to avoid collecting data (e.g., by keeping the data local on your device), nor to avoid associating information with you (as Apple sometimes does). Furthermore, some personal information that Facebook collects is unlikely to be used for service-related purposes at all. For example, it is not credible that Facebook has service-related purposes for much of the extensive and detailed information it collects about your devices and about other applications you utilize.

---

a definition similar to (but not exactly the same as) the CCPA definition; see Facebook, "California Privacy Notice" (Facebook California), July 1, 2020, https://www.facebook.com/legal/policy/ccpa. Twitter interchangeably uses the terms *personal information* and *personal data*, but does define them. Pinterest uses the term *personal information*, but does not define it.

[271] Facebook at "Device information".

[272] Facebook at "Provide, personalize and improve our Products".

[273] Facebook at "Provide, personalize and improve our Products".

[274] Facebook at "Information across Facebook Products and devices".

[275] Facebook at "Face recognition".

[276] Pinterest at "What we do with the info we collect".

[277] Twitter at "Location Information".

Like Google, non-service-related purposes principally consist of advertising. As with Google, advertising is Facebook's, Twitter's, and Pinterest's principal business, and their services are often free to consumers. Consequently, these social networks use much of the personal information they collect for behavioral advertising. Facebook uses "the information we have about you - including information about your interests, actions and connections - to select and personalize ads, offers and other sponsored content that we show you."[278] Similarly, Twitter uses "[y]our activity on Twitter, the information you provide to Twitter, and our relationships with ad partners" to "help make promoted content more relevant for you"[279], and Pinterest uses "your interests based on your onsite and offsite activities" and "information we receive from ad partners or other third parties" to "[d]ecide which ads to show you."[280] These social networks also location information they collect for location-based advertising. Facebook uses "location-related information - such as your current location, where you live, the places you like to go, and the businesses and people you're near - to provide, personalize and improve our Products, including ads"[281], and Twitter uses location to "personalize our services including with more relevant content like local trends, stories, ads, and suggestions for people to follow"[282].

Facebook gives examples of the types of personal information that it uses for advertising, and these examples show that the personal information used is extensive and detailed. Ads are "based on your activity across Facebook companies and products - such as [p]ages you and your friends like", "[i]nformation from your Facebook and Instagram profile", and "[p]laces you check in using Facebook".[283] Ads are also based on information obtained through Facebook's online advertising platform, including "[w]ebsites you visit or apps you use [that] send Facebook data", including "[a]dding a product to a shopping cart

---

[278] Facebook at "Ads and other sponsored content".

[279] Twitter, "How Twitter Ads work" (Twitter Ads), undated, accessed October 20, 2020, https://business.twitter.com/en/help/troubleshooting/how-twitter-ads-work.html, at "Why you see certain Twitter Ads".

[280] Pinterest at "What we do with the info we collect".

[281] Facebook at "Location-related information".

[282] Twitter at "Location Information".

[283] Facebook, "Understand what data is used to show you ads" (Facebook Ads), undated, accessed November 16, 2020, https://www.facebook.com/ads/about/ at "Your activity across Facebook companies and products".

or making a purchase".[284] Ads are also based on information obtained through Facebook's offline advertising platform, including "purchases at retail stores", because "[w]hen you share information like your phone number or email address with a business, they might add it to a customer list that can be matched to your Facebook profile."[285]

However, unlike Google, Microsoft, and Apple—each of which discloses types of user content that are *not* used for advertising—Facebook does not disclose whether it uses content provided by users (potentially including your communications) for behavioral advertising. Indeed, Facebook states that it "automatically process[es] content and communications you and others provide to analyze context and what's in them" for "the purposes described" in its privacy policy, which includes advertising.[286] We expect that many users would be surprised to learn that Facebook may be examining the content of their private communications with other Facebook users, and using what it finds for targeted advertising. In contrast, Twitter states that it does not use certain sensitive categories (e.g., "race, religion, politics, sex life, or health") for advertising[287], and it does not use the content of direct messages for advertising.[288]

D. Sharing

Like others, Facebook, Twitter, and Pinterest share personal information with both service providers and third parties.

Unfortunately, Facebook neither distinguishes in its disclosures between service providers and third parties, nor provides the information about contractual provisions that would allow us to determine which are service providers. Some of the purposes for which Facebook shares personal information are similar to the purposes for which application suites share personal information with *service providers*, including "analytics and measurement reports", and "technical infrastructure services, analyzing how our Products are used, providing customer service, facilitating payments or conducting surveys".[289] However, whereas other companies often accompany such disclosures

---

[284] Facebook Ads at "Your activity on other websites and apps".

[285] Facebook Ads at "Your activity with other businesses".

[286] Facebook at "Things you and others do and provide".

[287] Twitter at "Advertisers and Other Ad Partners".

[288] Twitter at "Direct Messages and Non-Public Communications".

[289] Facebook at "Measurement partners" and "Vendors and service providers".

of sharing with a statement about the nature of contractual limits on the use of such shared personal information, Facebook merely states that it "impose[s] strict restrictions on how our partners can use and disclose the data we provide".[290]

In contrast, Twitter discloses a list of service providers[291], and states that its service providers are subject to "obligations consistent with this Privacy Policy" and that shared personal information is used by them "only on our behalf"[292].

Each social network also shares personal information at a user's direction and with user consent to construct the social network. A user's privacy settings determine if Facebook shares the user's posts, lists of friends, communications, and "engagement with ads and sponsored content" with only friends, with a particular business, or with the public.[293] However, somewhat unique to social networks, Facebook makes easy for your friends "who can see your activity on our Products ... to share it with others", e.g. "when you comment on someone else's post or react to their content, your comment or reaction is visible to anyone who can see the other person's content".[294] It is unclear whether users who share posts only with friends realize that their comments are visible to people other than their friends. In contrast, Twitter shares Tweets other than "protected Tweets and Direct Messages" with the public, regardless of a user's privacy settings.[295] In a blend of Facebook's and Twitter's practices, Pinterest shares "public boards and Pins" with the public, but only shares "secret boards" with those you or another collaborator invite to view them.[296]

In its advertising business, Facebook's sharing may resemble Google's. Since Facebook similarly has its own advertising platform, it does not need to share personal information in order for advertisers to place ads based on audience segments.[297] In contrast, Twitter and Pinterest share personal information with advertisers. Twitter's sharing

---

[290] Facebook at "Sharing with Third-Party Partners".

[291] Twitter, "Our Service Providers" (Twitter Service Providers), undated, accessed October 20, 2020, https://privacy.twitter.com/en/subprocessors.

[292] Twitter at "Service Providers".

[293] Facebook at "People and accounts you share and communicate with"..

[294] Facebook at "Content others share or reshare about you".

[295] Twitter at "You should read this policy in full, but here are a few key things we hope you take away from it".

[296] Pinterest at "How and when we share information".

[297] Facebook at "Advertisers".

with advertisers appears to be the combination of a personal identifier (e.g., email address, mobile device identifier), audience segments (e.g., "if you search for a specific term, we may show you promoted content related to that topic"), and particular brands or businesses (e.g., "you could receive a Promoted Tweet about a deal or promotion from a business whose website you frequent, or email newsletter you subscribe to").[298] Pinterest's sharing with advertisers appears to be the combination of a personal identifier with audience segments (e.g., "if you show an interest in camping tents on Pinterest, we may show you ads for other outdoor products").[299]

However, Facebook's sharing of personal information with third parties is distinctively unique, because Facebook integrates third-party apps into its social network. When you use a third-party app, the third party "can receive information about what you post or share".[300] As an example, Facebook states that "when you play a game with your Facebook friends ... the game developer ... can receive information about your activities in the game".[301] The third party may also "receive your list of Facebook friends".[302] But the sharing with third-party apps doesn't stop there. Facebook's privacy policy allows it to share any "information about what you post or share", not only that related to the third-party app. We doubt that users are aware, when they use a third-party app inside Facebook, that the third-party app has access to their posts. In addition, in the past, Facebook allowed such third parties to receive additional information about your friends; but now it guarantees that it does not.[303] Facebook also shares personal information that it collects outside its social network with third parties. When you use a third-party website that integrates a Facebook product (e.g., a Facebook Like button, a Facebook login, or perhaps merely a Facebook Pixel[304]), the third party "can receive information about what you post

---

[298] Twitter Ads at "Why you see certain Twitter Ads".

[299] Pinterest at "What we do with the info we collect".

[300] Facebook at "Apps, websites, and third-party integrations on or using our Products".

[301] Facebook at "Apps, websites, and third-party integrations on or using our Products".

[302] Facebook at "Apps, websites, and third-party integrations on or using our Products".

[303] Facebook at "Apps, websites, and third-party integrations on or using our Products".

[304] Facebook at "Information from partners".

or share".[305] Facebook gives as an example that "when you ... use a Facebook Comment or Share button on a website, ... the website ... can receive a comment or link that you share from the website on Facebook".[306] In addition, Facebook's privacy policy also allows it to share any "information about what you post or share", not only that related to the third- party website. We doubt that uses are aware, when they click on a Facebook Like button, that they are giving access to the third-party website on which it appears access to all of their posts.

Twitter also integrates third-party apps into its social network.[307] Such third-party apps can access public personal information on Twitter.[308] Third-party apps that are capable of sending or receiving Direct Messages can also access this type of private personal information, upon approval of the user, but they are prohibited from "[s]haring or publishing protected content, or any other private or confidential information".[309] Pinterest offers a more limited integration of third-party apps.[310] Such third-party apps can only access public personal information on Pinterest[311], and in addition they are prohibited from using this personal information "to target people with advertising outside of Pinterest".[312]

Facebook's sharing of personal information is quite different than that of Google, Microsoft, or Apple. Both Google's and Apple's sharing of personal information with third parties is much more limited. Whereas Microsoft shares more personal information than does Facebook for advertising (since Microsoft does not have its own advertising platform), Facebook shares much more personal information

---

[305] Facebook at "Apps, websites, and third-party integrations on or using our Products".

[306] Facebook at "Apps, websites, and third-party integrations on or using our Products".

[307] Twitter,"AboutTwitter'sAPIs"(TwitterAPIs),undated,accessedOctober23,2020, https://help.twitter.com/en/rules-and-policies/twitter-api.

[308] Twitter APIs at "Accessing Twitter Data".

[309]Twitter,"TwitterDeveloperPolicy"(TwitterApps),undated,accessedOctober23, 2020, https://developer.twitter.com/en/developer-terms/policy, at "Consent & permissions".

[310] Pinterest,"DeveloperandAPITermsofService"(PinterestApps),May4,2020, https://developers.pinterest.com/terms/.

[311] Pinterest Apps at "Your responsibilities regarding privacy".

[312] Pinterest, "Developer Guidelines" (Pinterest APIs), undated, accessed October 23, 2020, https://policy.pinterest.com/en/developer-guidelines, at "Accessing APIs".

with third parties through third-party social network apps and through website tools.

E. User Choice

Facebook, Twitter, and Pinterest afford users few choices over *collection* of personal information, but substantial choices over *use* and *sharing*.

With respect to *collection* of personal information, Facebook affords users few choices, other than by not putting such information into Facebook products in the first place. Facebook does give users the ability to opt-out of Facebook's creation of the user's location history.[313] Twitter gives users the ability to opt-out of Twitter's collection of "websites where you see Twitter content".[314] Pinterest honors the Do Not Track browser setting, and if the setting is on Pinterest does not collect data off of Pinterest.[315] Other than these few choices, we found no other choices about collection in Facebook's, Twitter's, or Pinterest's privacy settings.

This stands in stark contrast to the application suites discussed above. Google (which also extensively collects personal information) affords users extensive choices, and Microsoft affords users some (but fewer) choices. Apple affords users no choices over collection, but it collects far less personal information than does Facebook. Whereas Apple architects some its products to leave personal information locally on user devices, Facebook does not. Facebook even collects the content of what users likely perceive as private communications between Facebook users.

With respect to *use* of personal information, Facebook, Twitter, and Pinterest afford users more choices. Facebook allows a user to opt-out of the use of your personal information for advertising to your friends and/or for advertising by Facebook on third-party websites and apps.[316] It also allows a user to opt-out of the use of personal information that Facebook obtains from third parties for advertising by

---

[313] Facebook, "Learn More About Your Android Location Settings", undated, accessed November 16, 2020, https://www.facebook.com/location_history/info.

[314] Twitter at "How You Control Additional Information We Receive".

[315] Pinterest at "Choices you have about your info".

[316] Facebook, "Your Ad Preferences" (Facebook Advertising), undated, accessed Nov. 16, 2020, https://www.facebook.com/ds/preferences/?entry_product=ad_settings_screen at "Social Interactions" and "Ads shown off of Facebook".

Facebook.[317] In contrast, Facebook does not afford a user a similar yes or no choice over whether your personal information can be used for advertising by Facebook to you in Facebook's own social network. It does, however, give a user the ability to opt-out of the use of particular categories of personal information for advertising by Facebook (e.g., relationship status, employer, job title, education, and audience segments that Facebook puts you into).[318] Facebook also allows a user to opt-in to the use of photos and videos for facial recognition.[319]

Twitter allows a user to opt-out of the use of personal information that Twitter collects from third parties for advertising on and off Twitter.[320] Twitter also allows a user to opt-out of the use of personal information that Twitter collects on Twitter while you are not logged into to Twitter.[321] However, Twitter does not afford a user a similar choice over whether your personal information collected on Twitter's service while you are logged in can be used for advertising on and off Twitter.[322]

Pinterest allows a user to opt-out of the use of personal information that Pinterest collects from third parties for advertising on Pinterest.[323] Pinterest also allows a user to opt-out of the use of personal information that Pinterest collects on Pinterest for advertising by Pinterest outside of Pinterest.[324] However, Pinterest does not afford a user a similar choice over whether your personal information collected on Pinterest's service can be used for advertising on Pinterest.

Curiously, Facebook's, Twitter's, and Pinterest's privacy controls are the opposite of the approach of Google, which allows users

---

[317] Facebook Advertising at "Data about your activity from partners".

[318] Facebook Advertising at "Categories used to reach you".

[319] Facebook, "What is the face recognition setting on Facebook and how does it work?", undated, accessed Nov. 16, 2020, https://www.facebook.com/help/122175507864081.

[320] Twitter, "Your privacy controls for personalized ads" (Twitter Personalization), undated, accessed Oct. 23, 2020, https://help.twitter.com/en/safety-and-security/privacy-controls-for-tailored-ads, at "What are my privacy options?".

[321] Twitter, "About personalization across your devices" (Twitter Inferred Identity), undated, accessed October 23, 2020, https://help.twitter.com/en/about-personalization-across-your-devices.

[322] Twitter Personalization at "What are my privacy options?".

[323]Pinterest at "Choices you have about your info".

[324] Pinterest at "Choices you have about your info".

choices over advertising on Google services but not on non-Google services that use the Google advertising platform.

With respect to *sharing* of personal information, Facebook, Twitter, and Pinterest again differ from the application suites. Whereas Apple and Microsoft afford users granular choices over the sharing of personal information with third parties through separate privacy settings for each app, Facebook only allows such granular choice when it comes to sharing personal information with friends or the public.[325] However, it affords users no such granular choice over sharing of personal information with third parties through third-party apps and websites that use Facebook Business products. Twitter affords users who are logged in a choice to opt-out of the sharing of non-public personal information ad brokers (e.g., Google and Facebook).[326] As a result, Facebook, Twitter, and Pinterest give users less control over sharing of personal information with third parties than do any of the application suite providers.

8. INTERNET SERVICE PROVIDERS (COMCAST, AT&T, AND COX)

A small number of Internet Service Providers (ISPs) provide broadband Internet service to the majority of the United States population. We consider Comcast (the ISP with the largest market share), AT&T (the ISP with the 3rd largest market share), and Cox (an ISP with a moderate market share).

A. Scope

Comcast, AT&T, and Cox each have a single privacy policy that applies to most of their services, including broadband Internet service, voice service, video services, and home services.[327] We focus

---

[325] Facebook, "Control Who Can See What You Share", undated, accessed November 16, 2020, https://www.facebook.com/help/1297502253597210.

[326] Twitter, "Additional information sharing with business partners" (Twitter Partners), April 6, 2020, https://help.twitter.com/en/safety-and-security/data-through-partnerships.

[327] Comcast, "Our Privacy Policy explained" (Comcast), June 30, 2020, https://www.xfinity.com/privacy/policy, at "When the Privacy Policy Applies"; AT&T, "AT&T Privacy Policy" (AT&T), June 19, 2020, https://about.att.com/csr/home/privacy/full_privacy_policy.html, at "When this

here only on broadband Internet services. Cox's privacy policy (unlike those of AT&T or Comcast) has portions that are specific to broadband Internet service.

B. Collection

Comcast and AT&T collect a similar range of personal identifiers as do Google, Microsoft and Apple, including contact information (e.g., name, address, and email address), device identifiers (unspecified), and advertising identifiers (e.g., Apple or Android advertising identifier).[328] Although Cox similarly collects contact information and device identifiers (e.g., IP address), Cox does not collect advertising identifiers.[329]

Comcast and AT&T collect a wide range of behavioral information based on their technical ability and the nature of broadband Internet service.

Some of the behavioral information focusses on apps and devices used by a consumer, as do all of the cases considered earlier in this paper to varying extents. AT&T collects information about the "mobile apps you use" and "the time you spend on ... apps".[330] Comcast collects "[d]evice ... information".[331]

Other behavioral information focusses on user interests. AT&T collects the "search terms you enter", "information regarding an individual's interaction with an internet website, application, or advertisement", "videos viewed", and "items identified in your online shopping carts".[332] Similarly (but more vaguely), Comcast collects "user activity information, including what you search ...".[333] Because the CCPA requires more granular disclosures for California residents, Comcast also

---

Policy applies"; Cox, "Your Privacy Rights as a Cox Customer and Related Information" (Cox), August 1, 2020, https://www.cox.com/aboutus/policies/annual-privacy-notice.html, at "Information We Collect?".

[328] Comcast at "The Personal Information We Collect and How We Collect It".; AT&T at "The information we collect".

[329] Cox at "Internet Services" within "Information We Collect?".

[330] AT&T at "Web browsing and app information".

[331] Comcast at "How We Collect Personal Information".

[332] AT&T at "Web browsing and app information" and at "California Consumer Privacy Act (CCPA)" under "Information We Collected From Consumers".

[332] Comcast at "How We Collect Personal Information".

[333] Comcast at "How We Collect Personal Information".

discloses that it collects "information regarding your interaction with an internet website, application, or advertisement".[334] However, the information about searches that an ISP may collect is limited, since searches are usually encrypted and thus not observable by ISPs.

Yet other behavioral information focusses on the sites a user visits on the Internet. AT&T collects "the websites you visit" and "the time you spend on websites".[335] Similarly, Comcast collects "Domain Name Server ... searches and network traffic activity"[336]. Because the CCPA requires more granular disclosures for California residents, Comcast also discloses that it collects "[b]rowsing history".[337] The information about the sites a user visits that an ISP may collect is extraordinarily broad, since an ISP uniquely has the technical ability to collect information about every site a user visits on the Internet, through observation of the IP header of packets and of DNS queries.

Similar to many cases considered earlier in the paper, AT&T and Comcast also collect information about a user's location, using information provided by cell towers and information provided by mobile devices (e.g., accessible Wi-Fi and Bluetooth networks and GPS information).

Cox's collection of personal information is considerably more limited than that of either AT&T or Comcast. Whereas AT&T and Comcast collect a wide variety of behavioral information, Cox only collects information about "the volume of and types of data transmitted and received through your service, ..., connection dates and times" and "the volume of data transmitted by certain protocols, devices and services".[338] Cox does not "read the contents of your online communications, such as email, unless required by law or court order."[339]

---

[334] Comcast at "Collection and Use of Personal Information" under "Learn more about your rights if you are a California resident and how to exercise them".

[335] AT&T at "Web browsing and app information".

[336] Comcast at "The Personal Information We Collect and How We Collect It".

[337] Comcast at "Collection and Use of Personal Information" under "Learn more about your rights if you are a California resident and how to exercise them".

[338] Cox at "Internet Services" within "Information We Collect?".

[339] Cox at "Use and Sharing?".

C. Use

As with other cases considered in this paper, the ISPs use this personal information[340] for both service- related and non-service-related purposes.[341]

Disappointingly, the service-related purposes are unspecified by each of the three ISPs. By the nature of broadband Internet service, they must include using the domain names and IP addresses of the Internet endpoints which users wish to visit in order to route their packets, and using mobile device location to maintain a connection to the cell network. However, it remains unclear whether there are service-related purposes for collecting other information on user behavior.

As with other cases considered in this paper, the principal disclosed non-service-related purpose is advertising. AT&T discloses that one of its subsidiaries (Xandr [342]) uses personal information for advertising.[343] Comcast, in its mandated CCPA disclosure, states that (unspecified) affiliates use personal information[344], and a little bit of

---

[340] Comcast defines *personal information* as "any information that is linked or reasonably linkable to you or your household"; see Comcast at "Introduction" in the popup window for *personal information.* Comcast states that *personal information* "can include information that does not personally identify you — such as device numbers, IP addresses, and account numbers" and "may also include information that does personally identify you, such as your name, address, and telephone number"; see Comcast at "The Personal Information We Collect and How We Collect It". AT&T uses the CCPA definition of *personal information.* Cox uses the term *Personally Identifiable Information* and defines it as "subscriber name, service and mailing addresses, telephone numbers, social security number, driver's license number, email address, billing and payment records (including credit card and bank account numbers used to pay for our services), subscriber credit information, or other information that potentially could be used to identify, contact, or locate you"; see Cox at "Your Information". Cox considers contact information to be *personally identifiable information*, but considers "general location, demographics, ..., usage, ... and preferences" to be *non-personally identifiable information* unless it is directly linked to *Personally Identifiable Information.*

[341] Comcast at "How and When We Use Information, Including for Marketing and Advertising"; AT&T at "How we use your information"; Cox at "Use and Sharing?".

[342] AT&T at "Affiliates".

[343] AT&T at "Sharing information across the AT&T affiliates".

[344] Comcast at "Learn more about your rights if you are a California resident and how to exercise them" under "Categories of Third Parties to Whom PI was 'Sold'".

digging reveals that one such affiliate is likely effectv (an advertising division of Comcast[345]).

It is frustratingly difficult to determine what personal information Comcast and AT&T use for advertising. Although Comcast collects "network traffic activity", its nationwide privacy policy states that "[w]here you go in the Internet is your business, not ours", and that Comcast "de-identif[ies] our customer's network traffic activity within 24 hours and then only use[s] that de-identified information" for network planning and "to improve our products and services".[346] Similarly, it states that Comcast has "never used [DNS] data for any sort of marketing or advertising". However, for California residents, Comcast discloses that it uses "[i]nferences drawn from other personal information" consisting of a "[p]rofile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" to "provide marketing and advertising".[347] This leaves open the question of what personal information Comcast collects, other than "network traffic data" and DNS requests, that enable it to create such a detailed profile.

In contrast, Cox's use of personal information[348] is much more limited than that of Comcast and AT&T, because Cox does not collect most of the behavioral information that Comcast and AT&T collect. Thus, while Cox also uses personal information for advertising, this personal information does not include either websites visited or user interests collected via the broadband service. For example, Cox uses "your general geographic area and nine-digit ZIP code" for "location-based online advertising".[349]

D. Sharing

All three ISPs share personal information with service providers.[350] The purposes for which AT&T shares personal information with

---

[345] effectv, "Who We Are", https://effectv.com/about.

[346] Comcast at "How and When We Use Information, Including for Marketing and Advertising".

[347] Comcast at "Collection and Use of Personal Information" under "Learn more about your rights if you are a California resident and how to exercise them".

[348] However, in this paper we use the term *personal information* as defined in the CCPA.

[349] Cox at "Use and Sharing?".

[350] Comcast at "When and With Whom We Share Information"; AT&T at "How we share your information"; Cox at "Use and Sharing?".

service providers includes "marketing or ad delivery services", "verifying or authenticating your identity, detecting fraud, protecting your financial accounts, and authorizing transactions".[351]

As with mobile apps for paid services, given that broadband service is a paid service, we expected their privacy policies to severely limit sharing of personal information with third parties. However, Comcast and AT&T, but not Cox, share personal information with third parties.[352]

The purposes for which AT&T shares personal information with third parties includes "advertising and marketing campaigns"[353] and "location services"[354]. AT&T shares both identifiers and behavioral information (including web browsing history and location) with third parties for both advertising purposes and location-based services.

It is frustratingly difficult to determine what personal information Comcast shares with third parties for advertising purposes. Comcast's privacy policy asserts that Comcast "do[es] not sell, and ha[s] never sold, information *that identifies who you are* to anyone."[355] However, Comcast clarifies that it "share[s] de- identified or aggregate information that in no way identifies you with third parties when those third parties commit to not re-identify that information or share it with others who may attempt to do so".[356] Since Comcast considers your IP address (and presumably behavioral information linked to your IP address) as "information that does not personally identify you", Comcast may very well consider such information as *de-identified.*

Thus, it remains unclear which behavioral information Comcast shares with third parties. The situation becomes even less clear with additional disclosures. Comcast uses "cookies to deliver personalized advertising to you when you visit other websites, including

---

[351] AT&T at "Sharing information with non-AT&T companies that provide services for us or for you" and at "Sharing information with non-AT&T companies to enable third party services to you".

[352] Comcast at "When and With Whom We Share Information"; AT&T at "How we share your information".

[353] AT&T at "Sharing information with AT&T affiliates and non-AT&T companies for advertising and marketing programs".

[354] AT&T at "Sharing information to support location services".

[355] Comcast at "How and When We Use Information, Including for Marketing and Advertising" (emphasis added).

[356] Comcast at "How and When We Use Information, Including for Marketing and Advertising", in a pop-up window for "identifies".

advertising based on the products and services you viewed on our Services."[357] In a separate disclosure about Comcast cookies, Comcast states that such cookies include "[t]argeted [a]dvertising [c]ookies" that "collect data about your website visits, your use of the Services, your preferences, and your interaction with advertisements across platforms and devices for the purpose of delivering targeted advertising content on and off the Services."[358] Furthermore, for California residents, Comcast discloses that it shares "[i]nformation regarding your interaction with an internet website, application, or advertisement" with "advertising networks".[359] Even as experts in reading privacy policies, we cannot make sense of these seemingly conflicting statements.

We expect that most consumers would be surprised and disappointed if their ISP is sharing their web browsing history and location with third parties for purposes of advertising.

In contrast, Cox shares personal information with service providers but not with third parties.[360]

E. User Choice

None of the three ISPs afford users any choice over *collection* of personal information.

All three ISPs afford users very limited choices over some types of *use* (and thus perhaps indirectly over the *sharing*) of personal information.[361] AT&T allows users to opt-out of the use of their personal information to determine whether the user is included in a variety of audience segments.[362] Such audience segments are used in AT&T behavioral advertising. Similarly, Comcast allows users to opt-out of the use of their personal information for behavioral advertising on Comcast websites and apps.[363]

---

[357] Comcast at "When and With Whom We Share Information".

[358] Comcast,"ComcastXfinityCookiesNotice"(Comcastcookies), https://www.xfinity.com/privacy/policy/cookienotice, December 16, 2019.

[359] Comcast at "Collection and Use of Personal Information" under "Learn more about your rights if you are a California resident and how to exercise them".

[360] Cox at "Use and Sharing?".

[361] Comcast at "The Choices You Have to Control Our Use of Personal Information"; AT&T at "Your Privacy Choices and Controls".

[362] AT&T at "Relevant Advertising".

[363] Comcast, "Digital Advertising", https://my.xfinity.com/digitalads, undated, accessed April 1, 2020.

AT&T also invites users to *opt-in* to the use of more detailed personal information (e.g. web browsing history) in a more granular fashion for AT&T behavioral advertising.[364] Cox affords users a choice to opt-out of location-based online advertising.[365] Both AT&T and Comcast only allow Californians to opt-out of the sharing of their personal information with third parties, because they are mandated to under the CCPA.[366]

These user choices pale in comparison to those offered by Google, Microsoft, and Apple.

9. IOT DEVICES (AMAZON, FITBIT, AND GOOGLE)

Internet-of-Things (IoT) devices are a rapidly growing and evolving market. We consider Amazon's devices (including Echo speakers, Echo displays, Ring home security, and Fire TV streaming), Fitbit's devices (including watches, trackers, and scales), and Google's devices (including Home speakers; Nest thermostats, home security, hubs, and routers; and Chromecast streaming).

A. Scope

Fitbit has a privacy policy that applies to its devices and services.[367] Amazon's devices are included in a single privacy policy that applies to all of Amazon's products and services.[368] However, Amazon also provides a supplementary privacy policy for its eero devices.[369] Similarly, Google's devices are included in Google's overall privacy policy, discussed above. However, Google also provides a separate

---

[364] AT&T at "Enhanced Relevant Advertising".

[365] Cox, "Opting Out of Location-Based Advertising", https://www.cox.com/residential/support/opting-out-of-location-based-advertising.html, undated, accessed November 16, 2020.

[366] AT&T at "California Consumer Privacy Act"; Comcast at "Learn more about your rights if you are a California resident and how to exercise them".

[367] Fitbit, "Fitbit Privacy Policy" (Fitbit), October 8, 2020, https://www.fitbit.com/us/legal/privacy-policy. Fitbit has entered into an agreement to be acquired by Google; however, currently Fitbit has its own privacy policy.

[368] Amazon,"AmazonPrivacyNotice"(Amazon),January1,2020, https://www.amazon.com/gp/help/customer/display.html?nodeId=201909010.

[369] Amazon, "Privacy for eero Devices, Applications and Services" (Amazon eero), February 28, 2020, https://eero.com/legal/privacy.

disclosure that applies to its devices.[370] We focus here only on those elements of privacy policies relevant to their IoT devices.

B. Collection

Amazon, Fitbit, and Google collect from these devices a similar range of personal identifiers as do many others discussed above (e.g., contact information, device identifiers, and advertising identifiers).[371]

Some, but not all, also collect behavioral information that focusses on apps and devices used by a consumer. Google collects from Wi-Fi routers "information about the types of connected devices you have and their network usage".[372] Amazon collects "device log files and configurations"[373], "performance statistics", "network bandwidth usage statistics", "device hostnames", "Application clickstream", "types of connected devices, the association of devices with a specific family profile, and WiFi signals from other WiFi systems in the area"[374]. In contrast, Fitbit does not appear to collect information about apps and devices other than its own.[375]

Similar to many cases considered earlier in the paper, the providers of these IoT devices also collect information about a user's location.[376]

Some IoT devices also collect behavioral information that focusses on user interests. Voice assistants (e.g., those embedded in Amazon and Google IoT devices) collect "content interaction information,

---

[370] Google, "Our commitment to privacy in the home" (Google Nest), undated, accessed November 16, 2020, https://store.google.com/us/magazine/google_nest_privacy.

[371] Amazon at "Examples of Information Collected" and Amazon eero at "Types of data we collect"; Fitbit at "Account Information", "Device Information", and "Usage Information"; Google at "Unique identifiers" and "We want you to understand the types of information we collect as you use our services", in the pop-up window for "personal information".

[372] Google Nest at "What is data from my Google Wifi router sent to Google, and how is it used?".

[373] Amazon at "Examples of Information Collected".

[374] Amazon eero at "Types of data we collect".

[375] Fitbit at "Device Information" and "Usage Information".

[376] Amazon at "Examples of Information Collected"; Fitbit at "Geolocation Information"; Google at "Your location information".

such as content downloads, streams, and playback details"[377] Such information may be similar to information collected by search providers and by ISPs.

The principal differences in data collection between these IoT devices and other cases considered above lies in other types of behavioral information.

These IoT devices collect much more audio, video, and sensor information than any other cases considered above. Fitbit collects "your logs for food, weight, sleep, water, or female health tracking".[378] Google collects audio[379], video[380], and sensor data "such as motion, whether or not someone is home, ambient light, temperature, and humidity"[381]. Amazon collects "voice recordings when you speak to Alexa" and "images and videos collected or stored in connection with Amazon Services".[382]

However, in some cases, the companies offering these IoT services commit to collecting much less information about the sites a user visits on the Internet than do others. Google does not collect from Wi-Fi routers "the websites you visit, nor does it monitor the content of traffic on your Wi-Fi network".[383] This stands in stark contrast to some ISPs that do.

C. Use

Service-related purposes are intimately tied to the specific purposes of each device. Fitbit uses "[b]iometric information, such as your exercise, activity, sleep, or health data, including the number of steps you take, distance traveled, calories burned, weight, heart rate, sleep stages, [and] active minutes"[384] to "provide you with your Fitbit

---

[377] Amazon at "Examples of Information Collected".

[378] Fitbit at "Additional Information".

[379] Google Nest at "Microphones".

[380] Google Nest at "Cameras".

[381] Google Nest at "Why does Google collect environmental and activity sensor data from my home, and how is it used?".

[382] Amazon at "Examples of Information Collected".

[383] Google Nest at "Wifi data".

[384] Fitbit at "Categories of Information We Collect, Use, and Disclose for Business Purposes".

dashboard"[385]. Google uses video for Nest Cam monitoring[386], audio for voice assistant functionality, and sensor data "across multiple Nest devices in your home to automatically switch the behavior of Nest devices in your home when you leave and when you come back"[387].

IoT services differ in which personal information they use for non-service-related purposes. Amazon users personal information to "[t]ailor our Products to your interests".[388] Amazon states that it "do[es] not use information which on its own identifies you, such as name or e-mail address, to serve interest-based ads".[389]

However, since this statement does not preclude using other types of personal information collected by its IoT devices for behavioral advertising, we must conclude that it may use such personal information "to display interest-based ads for features, products, and services that might be of interest to you".[390]

In contrast, Google guarantees that it does not use "your video footage, audio recordings, and home environment sensor readings" or "Wi-Fi network performance data" for "ad personalization".[391] It does, however, use interaction with its voice assistant to "inform your interests for ad personalization", namely to put you into an audience segment. For example, if you ask, "Hey Google, what's the weather today?", then Google may "use the text of that voice interaction (but not the audio recording itself) to show you personalized ads".[392] Fitbit discloses granular information about some types of personal information used for advertising, but fails to provide any clear statement about whether its uses sensor data for such purposes.[393]

---

[385] Fitbit at "How We Use Information".

[386] Google Nest at "Cameras".

[387] Google Nest at "Why does Google collect environmental and activity sensor data from my home, and how is it used?".

[388] Amazon eero at "Use of your Personal Data".

[389] Amazon,"Interest-BasedAds"(Amazonads),undated,accessedJune5,2020, https://www.amazon.com/gp/help/customer/display.html?nodeId=202075050.

[390] Amazon at "For What Purposes Does Amazon Use Your Personal Information".

[391] Google Nest, including at "Wifi data".

[392] Google Nest.

[393] Fitbit at "Analytics and Advertising Services Provided by Others"; Fitbit "Cookies on the Fitbit Services" (Fitbit Cookies), undated, accessed April 21, 2020, https://www.fitbit.com/us/legal/cookie-list.

D. Sharing

Like others discussed above, IoT services share some personal information with service providers.[394] Like others discussed above, they may also share personal information with third parties for user-directed purposes.[395]

Beyond such purposes, IoT services differ in what personal information (if any) they share with third parties. Amazon appears to share only a personal identifier paired with audience segments.[396] Fitbit appears to not directly share any personal information[397]; however, it appears to enable advertising platforms to directly collect some personal information that allows advertising based on audience segments.[398] As discussed above, Google does not appear to share any personal information, since Google's advertising platform does not require such sharing in order for advertisers to place ads based on audience segments.

Thus, although the types of personal information collected by these IoT devices is often considered sensitive, it appears that little of it is likely shared with third parties. This stands in contrast to others considered above.

E. User Choice

Some IoT devices afford users choices over which personal information is *collected* and when. Google devices collects audio only "if we detect that you or someone in your home is interacting with your Assistant"[399] and collects video only "if you or someone in your home has explicitly turned the camera on or enabled a feature that needs it"[400]. Google also allows users to opt-out of the collection of certain

---

[394] Amazon at "Third-Party Service Providers"; Fitbit at "For External Processing"; Google at "For external processing".

[395] Amazon at "Transactions involving Third Parties"; Fitbit at "When You Agree or Direct Us to Share"; Google at "With your consent".

[396] Amazon at "Does Amazon Share Your Personal Information?" and "What About Advertising?".

[397] Fitbit at "How Information is Shared".

[398] Fitbit Cookies.

[399] Google Nest at "Microphones".

[400] Google Nest at "Cameras".

information about device usage.[401] Fitbit gives user choices over which logs are collected.[402] These choices exceed those offered by Facebook and by ISPs.

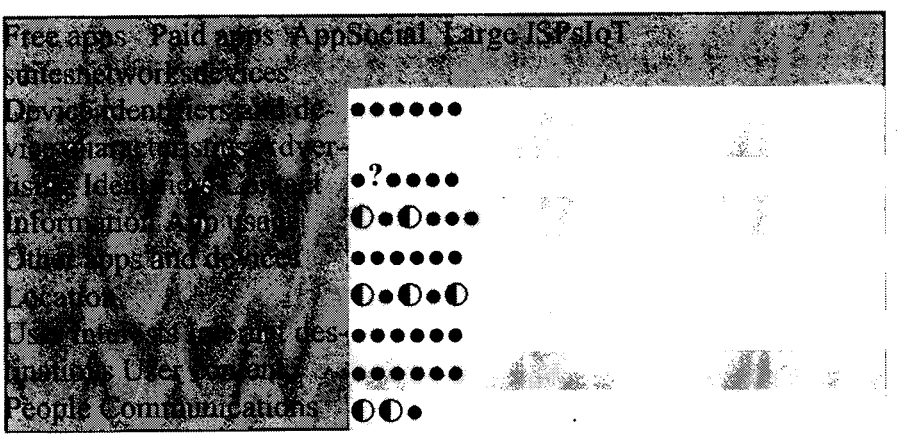
IoT devices also afford users some choices over some types of *use* and/or *sharing* of personal information. Amazon allows users to opt-out of behavioral advertising altogether, but it gives no granular choices over which personal information is used for behavioral advertising if allowed.[403] As discussed above, Google allows users to opt-out of the use of personal information for ad personalization on Google services, but not out of the use of personal information for ad personalization on non-Google services that use the Google advertising platform.

10. COMPARISONS AND CONCLUSIONS

In each section above, we compared the privacy policies of each company to others in its category and to those in different categories. Here, we collate these comparisons and make some concluding observations.

A. Collection and Use for Service-Related Purposes

Collection of personal information is summarized in Table 1.



[401] Google, "Google Nest Wifi and your privacy", October 15, 2019, https://support.google.com/wifi/answer/6246642, at "Information collected".

[402] Fitbit at "Account Information".

[403] Amazon at "What Choices Do I Have?".

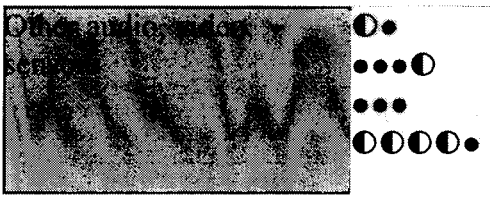


Table 1: Collection of Personal Information (● = all collect; ◐ = some collect; ? = not sure; blank = none collect)

All companies we examined collect device identifiers. The device identifiers are usually unspecified, but typically include (at a minimum) the IP address of the device a consumer is using, and the IMEI (if the device has a cellular radio). Device identifiers are commonly used for service-related purposes, including tailoring the user interface to the type of device and operating system.

Almost all (or all) companies collect advertising identifiers, including those assigned on mobile devices running either the Apple or Android operating systems. However, advertising identifiers are rarely used for service-related purposes.

Applications which are intended to be used while logged into an account collect contact information. This includes all of the applications we considered, except for a few of the free apps and for application suites that may be used without logging in. The account is commonly used to enable access to private content, personalization of the service, synchronization between multiple devices, and purchases.

All companies collect information about the usage of their own application or service. This information is often used for maintaining the product and for future product development. Sometimes aggregated forms of this information are used for billing, e.g. when there is usage-based pricing.

Some—but not all—of the companies collect information about the other applications and devices that consumers use. Amongst those we examined, it is generally the larger companies that collect such information. Sometimes, information about other devices is used for service-related purposes. A prominent example is an application or device that communicates with other devices inside the home, including routers and smart home devices. However, sometimes we cannot identify any technical reason for this collection. This distinction is important. For example, the GDPR only allows a business to mandate in terms and conditions collection of personal information that is technically necessary for the performance of the contract between the user and the business.

All companies collect information about location. The location is often used for service-related purposes to customize the content provided to the user. For example, a weather app can display local weather, a ride- sharing app can find the customer and track the ride, and maps can offer turn-by-turn directions.

All companies collect some type of information related to user interests. The information from which these user interests are derived almost always come from the manner in which consumers utilize the service or application. Sometimes the information is used to implement that functionality. For example, search engines collect user interests in order to provide search results.

Only a few companies have the technical ability to widely track the sites you visit on the Internet. These include ISPs, which have the ability to see every site you visit, and large advertising platforms (notably, Google and Facebook) whose tracking tools are present on a large percentage of websites. However, there are few service-related purposes for collecting and using such information, with the notable exception of security.

Some services—most notably application suites and social networks—offer users the ability to create and store content. Sometimes, this content is stored locally, but sometimes it is stored in the cloud. When stored in the cloud (e.g., Google Drive, Microsoft OneDrive, and Apple iCloud), such storage constitutes a service- related functionality. Social networks are constructed using user content, and further use content viewed to personalize the view each user has. Sometimes access to content enables additional functionality, e.g., adding events from email to a calendar.

Some services offers users the ability to communicate with other people. In this case, the service must use the identity of the other people and the content of the communication to transmit messages. ISPs must use the header of a packet to route it. Other common examples include email, texting, VoIP, and video conferencing.

Finally, some services—notably application suites, social networks, and IoT devices – collect audio, video, and/or sensor data for reasons other than communications with other people. These are collected for service- related functionalities particular to the service. For example, voice assistants use voice to respond to queries and commands, videocams use video for monitoring, and fitness IoT devices uses sensor data to provide a fitness dashboard.

B. Collection, Use, and Sharing for Advertising Purposes

Use of personal information for advertising is summarized in Table 2, and sharing of personal information is summarized in Table 3.

	Free apps	Paid apps	App suites	Social Networks	Large ISPs	IoT devices
Audience segments	◐	●	●	●	●	●
Location	●	●	●	●	●	●
Fine-grained user interests	◐	?	?	●	?	?
Internet destinations			◐	●	◐?	
User content	●					
People			?	●	?	?
Communications			◐?	◐	?	
Other audio, video, sensors				◐		◐?

Table 2: Use of Personal Information for Advertising (● = all use; ◐ = some use; ? = not sure; blank = none use)

Advertising identifiers and users' interests are used to create audience segments. The masters of this practice are those companies that also operate their own advertising platforms, most notably Google and Facebook. They create a large number of audience segments that span multiple dimensions; collect and integrate all personal information to which they have access; and then match this collated personal information to the audience segments. However, because these advertising platforms offer advertisers the ability to advertise to audience segments, all (or almost all) of the companies we examined also collect personal information using their own service or application and match this personal information to audience segments.

Some companies, e.g., Apple, collect personal information and match it to audience segments only in order to offer their own advertising. In this case, the company does not need to share personal information with third parties for this purpose. However, many companies also share combinations of the personal identifiers and audience segments of their users for third party advertising. Not surprisingly, the

providers of advertising-supported mobile apps do this to generate advertising revenue. However, quite surprising to us, the providers of mobile apps for paid services also commonly share with third parties personal identifiers paired with audience segments. We were similarly disappointed by the practices of large ISPs (e.g., AT&T and Comcast) that also share combinations of the personal identifiers and audience segments of their users for third party advertising. After all, these companies are paid substantial sums for their services, and we do not believe that users expect that their personal information is being shared with third parties for non- service-related purposes.

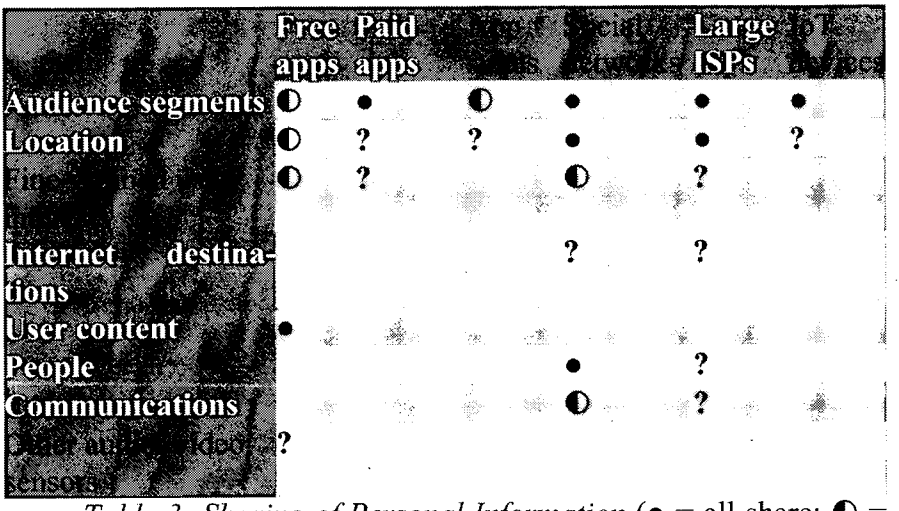


Table 3: Sharing of Personal Information (● = all share; ◐ = some share; ? = not sure; blank = none share)

Location information is used by all companies we examined for location-based advertising. Some companies use location information only for their own advertising, and thus do not share it with third parties. However, we were again disappointed to find that some large ISPs share location information with third parties. We were also frustrated that, in many cases, we are unable to determine whether location is shared with third parties. After all, the CCPA requires that a business disclose the categories of personal information shared with third parties.

Beyond using behavioral information to create audience segments, we found that some companies use fine- grained user interests that they collect for advertising. Unsurprisingly, this includes Facebook, which appears to use the wide-ranging and detailed information that it collects about user interests in a far more detailed manner for

advertising than just to create a broad set of audience segments. It also includes some advertising-supported apps. For example, KAYAK collects information about your searches, and shares that detailed information with third parties. This might surprise many users of KAYAK's mobile app, who may not expect that such detailed and personal information is being widely shared. We were also frustrated that, in many cases, we are unable to determine whether fine-grained user interests are used for advertising, and if so whether they are shared with third parties. In particular, we are unable to determine whether Chase, Uber, and United use (and perhaps even share) fine-grained information for advertising purposes. We were similarly unable to determine whether AT&T and Comcast use (and perhaps even share) fine-grained information or only audience segments for advertising. We found this surprising, given the sensitivity of the personal information that these companies collect, including financial and travel information.

Part of the problem may be that the GDPR and the CCPA only require a business to disclose the categories of personal information collected and shared, and these companies disclosures are too vague to determine how fine-grained this information is. Another part of the problem is that, although the GDPR and the CCPA have requirements about disclosure of collection and disclosure of use, privacy policies typically do not disclose the use of each particular category of personal information collected.

Information about the sites you visit on the Internet is a unique type of personal information that only a few companies have access to. ISPs must examine such personal information to offer broadband service. However, we were disappointed that AT&T may use web browsing history for advertising and may even share it with third parties. We were frustrated that we cannot rectify Comcast's conflicting statements about whether it similarly does so.

Although both application suites and social networks offer users the ability to create and store content, almost all state that they do not use this content for advertising purposes. For example, Apple, Google, and Microsoft all make such promises. However, we were appalled that Facebook may scan user content for advertising purposes.

Similarly, although a number of services offers users the ability to communicate with other people, we expected that such communications—whether by voice, email, text message, or video conferencing—would be strictly private. In some cases (e.g., in Apple's and Microsoft's privacy policies), we found clear statements that the company would not use such communications for advertising. However, we

were surprised and frustrated that in many cases, we found no such clarity. For example, we surely expected to find (but did not find) a prohibition on using communications for advertising in the privacy policies of all ISPs, given that they also offer telephone services, for which the law restricts similar behavior. And we were especially appalled that Facebook may scan user communications for advertising purposes.

Finally, we expected similar strict prohibitions on the use of other audio, video, and sensor data for advertising. We were pleased to see explicit statements by Apple and Microsoft that such information is not used for advertising. We were pleased to see similar statements by Google about raw audio, video, and sensor data, but disappointed that it may use the text of audio collected by its voice assistant to construct audience segments. And again, we were appalled that Facebook does not place even these types of personal information off limits for advertising purposes.

C. User Choice

User choices over collection, use, and sharing of personal information are summarized in Table 4.

Unsurprisingly, some advertising-supported mobile apps make collection, use, and sharing of personal information a take-it-or-leave-it proposition for using the app.[404] After all, the use and sharing for advertising purposes is likely the dominant source of revenue for some such apps.

More surprisingly, some mobile apps for paid services also make collection, use, and sharing of personal information a take-it-or-leave-it proposition for using their services. While collection and use for service- related functionality of the app is naturally a take-it-or-leave-it proposition for functionality that requires this personal information, we expected to find no sharing of personal information with third parties, or, at a minimum, that users would surely have the ability to control any such sharing. However, we found that some such mobile apps give users no such choices.

The CCPA requires that users be afforded an opt-out choice of their personal information being shared with third parties. Thus, some mobile apps that share personal information at least afford Californians

---

[404] We do not opine on when such take-it-or-leave-it propositions are consistent with the GDPR.

this choice. However, the CCPA does not require that users be afforded an opt-out choice of their personal information being collected and used by a business, and thus we often see that apps and service provide no such choices.

	Free apps	Paid apps	App Suites	Social Networks	Large ISPs	IoT Devices
Collection	□	□	◑	◑	□	◑
Use	◑	□	◑	◑	◑	◑
Sharing	◑	◑	□	◑	◑	◑

Table 4: User Choice over Collection, Use, and Sharing of Personal Information (□ = many choices; ◑ = some choices; □ = no choices)

Application suites provide users with more choices. However, our initial expectation—that those companies that collect less data would give users more choices over collection, use, and sharing of personal information – was wrong. Google affords users extensive choices over collection of personal information, but few choices over the use of such information once collected. Microsoft affords users fewer choices over collection, but extension choices over use and sharing. Apple affords users no choice over collection, few choices over use, and extensive choices over sharing. Overall, each offers users more choices than do mobile apps, but each in its own distinctive way, likely based on each's distinctive revenue streams.

Facebook, which has arguably the widest scope of types of personal information collected and the worst use and sharing practices, affords users few choices over collection but substantial choices over use and sharing. The only way that users can prohibit Facebook from collecting personal information is not to put that information into Facebook products in the first place. However, users can opt-out of the use and sharing of this personal information for advertising on third-party website and apps, but not on Facebook itself.

Large ISPs afford users no choice over collection, but give users the choice to opt-out of the use of their personal information for placing them into audience segments for advertising on their own sites, but no similar choice over sharing with third parties for advertising on third-party sites (except, as mandated, for Californians). As with mobile apps for paid service, while collection and use for service-related functionality of the app is naturally a take-it-or-leave-it proposition for functionality that requires this personal information, we expected to find no sharing of personal information with third parties, or, at a minimum, that users would surely have the ability to control any such

sharing. We found this lack of user choice over use and sharing for advertising profoundly disappointing, particularly given the paid nature of the service and the few (or no) options that consumers have to choose amongst broadband providers.

Finally, providers of IoT devices are uneven about user choice. Some given users more choices over collection than does Facebook or ISPs, principally choices over collection of audio, video, and sensor data. But they typically give users only limited choices over use and sharing for advertising.