




9-15-2021

## Risky Fine Print: A Novel Typology of Ethical Risks in Mobile App User Agreements

Bar Fargon Mizrahi

Follow this and additional works at: <https://digitalcommons.law.villanova.edu/vlr>

 Part of the [Computer Law Commons](#), [Consumer Protection Law Commons](#), [Contracts Commons](#), and the [Science and Technology Law Commons](#)

---

### Recommended Citation

Bar F. Mizrahi, *Risky Fine Print: A Novel Typology of Ethical Risks in Mobile App User Agreements*, 66 Vill. L. Rev. 483 (2021).

Available at: <https://digitalcommons.law.villanova.edu/vlr/vol66/iss3/1>

This Article is brought to you for free and open access by Villanova University Charles Widger School of Law Digital Repository. It has been accepted for inclusion in Villanova Law Review by an authorized editor of Villanova University Charles Widger School of Law Digital Repository.

---

---

# VILLANOVA LAW REVIEW

VOLUME 66

2021

NUMBER 3

---

---

## Articles

### RISKY FINE PRINT: A NOVEL TYPOLOGY OF ETHICAL RISKS IN MOBILE APP USER AGREEMENTS

BAR FARGON MIZRAHI\*

#### ABSTRACT

Mobile app users e-sign terms of service (ToS) and privacy policy agreements (PPA) on a daily basis, oftentimes without reviewing them. This practice is problematic because ToS and PPA include considerable “ethical risks,” that are, questionable elements that they would not reasonably expect to find in these agreements.

This Article introduces a novel conceptual framework and comprehensive typology for analyzing ethical risks in ToS and PPA of mobile apps. The proposed typology is the first to integrate ethical risks stemming from both ToS and PPA into a single coherent framework. Furthermore, the typology addresses the identified risks in terms of both the rights violated and the concrete business and legal practices that create them. Based on this thorough analysis, the Article argues that the legal mechanisms of ToS and PPA do not achieve their purposes. ToS and PPA often legalize ethical risks by obtaining users’ consent to terms that users may not fully understand. As such, rather than protecting users, ToS and PPA frequently perpetuate users’ vulnerabilities and subject them to rights-infringing measures.

---

\* Research fellow at the BIU Innovation Lab for Law, Data-Science, and Digital Ethics at Bar-Ilan University Faculty of Law. For helpful comments and suggestions, I thank Nofit Amir, Ittai Bar-Siman-Tov, Ariel Bendor, Ittai Cohen, Yuval Feldman, Shalhevet Hetli, Hadas Raichelson, Ayelet Sela, Sharon Shenhav, Bart van der Sloot, Yuval Zilber, and the participants of the International Conference on Law, Artificial Intelligence and Data Science: Challenges and Opportunities, at Bar-Ilan University, and of the International Machine Lawyering’s 2021 Conference, “Human Sovereignty and Machine Efficiency in the Law” at Chuck Law, the Chinese University of Hong Kong. This study was awarded a Best Paper Prize at the Machine Lawyering’s 2021 Conference and research grants from the Ministry of Science and Technology (Grant No. 3-15723), the Israel Council for Higher Education, and the Data Science Institute at Bar-Ilan University.

(483)

In addition, the Article examines the scope of protection against the identified ethical risks that is awarded by landmark laws in the area of digital privacy and consumer protection: The General Data Protection Regulation (GDPR), the Consumer Rights Directive of the European Union (EU), the California Consumer Privacy Act (CCPA), and the California Privacy Rights Act (CPRA).

The Article concludes with a discussion of its practical implications, which can have far-reaching consequences for privacy protection and consumer protection regulation. These implications include guidance for developing new regulatory and decision-support tools, improving consumer understanding of ethical risks, and assisting mobile app providers in drafting ethical user agreements.

2021] RISKY FINE PRINT 485

CONTENTS

INTRODUCTION .....	487
I. FRIEND OR FOE? MOBILE APP AGREEMENTS AS REGULATORY MECHANISMS FOR PROTECTING USERS' AUTONOMY .....	489
II. ETHICAL RISKS OF MOBILE APPS .....	494
A. <i>Ethical Risks Arising from the Content of ToS and PPA</i> .....	494
B. <i>Ethical Risks That Stem from Users' Lack of Informed             Decision-Making Regarding ToS and PPA</i> .....	495
1. <i>The Term "Privacy Policy" Misleads Users Into Thinking                 That Their Privacy Is Protected</i> .....	495
2. <i>Users Do Not Read the Terms of Service and Privacy                 Policy Agreements</i> .....	496
3. <i>Users Do Not Attribute Adequate Weight to the Cost of                 Privacy Violations</i> .....	496
C. <i>Ethical Risks That Are External to ToS and PPA</i> .....	497
1. <i>Information Security Failures</i> .....	497
2. <i>Identity Theft</i> .....	498
3. <i>Online Manipulation Based on Collected (and                 Transferred) Data</i> .....	498
III. NOVEL TYPOLOGY OF ETHICAL RISKS ARISING FROM THE CONTENT OF ToS AND PPA .....	499
A. <i>Methodology</i> .....	499
B. <i>Analysis and Results: The Ethical Risks Typology</i> .....	500
1. <i>Uninformed Consent</i> .....	501
a. <i>Unspecific Consent to the Service Provided</i> ...	503
i. <i>Broad Purpose Limitation</i> .....	503
ii. <i>Lack of Transparency</i> .....	504
b. <i>Limited User Data Control</i> .....	506
i. <i>Inability to Delete User Account Data</i> ....	506
ii. <i>Inability to Condition Over a Specific                         Clause</i> .....	507
iii. <i>Content Removal Clause</i> .....	507
iv. <i>Unilateral Termination Clause</i> .....	508
v. <i>Unilateral Change Clause</i> .....	508
vi. <i>Unilateral Changes of Financial Charges</i> ...	509
2. <i>Restricting User Legal Action</i> .....	510
a. <i>Mandatory Arbitration</i> .....	510
b. <i>Choice of Law</i> .....	511
c. <i>Choice of Jurisdiction</i> .....	511
d. <i>Limitation of Liability</i> .....	512
3. <i>Limited Readability</i> .....	512
a. <i>Ambiguity</i> .....	513
b. <i>Complexity</i> .....	514
c. <i>Length</i> .....	514
d. <i>Misleading or Unclear Language</i> .....	514

e. Difficulty of Navigation .....	515
4. <i>Profiling</i> .....	515
a. Creation of User Profiles that Negatively Affect Future Opportunities .....	516
b. Personal Information that May Be Used to Discriminate .....	517
c. Using Profiles for Undeclared Purposes .....	518
d. Creation of Aggregated Profiles .....	518
5. <i>Processing User Information</i> .....	518
a. Transforming Meta-Data Into Significant User Information .....	520
b. Aggregating and Combining User Information From Multiple Sources .....	521
6. <i>Tracking User Information</i> .....	522
a. Tracking User Activities While Users Are Not Using the App (Cookies) .....	522
7. <i>Third-Party Data Transfers</i> .....	523
IV. DISCUSSION AND APPLICATIONS .....	524
CONCLUSION .....	527

## INTRODUCTION

IN today's digital era, mobile devices and digital applications (apps) have become an indispensable part of everyday life. These apps have made many things simpler and more accessible. At the same time, mobile apps have inherent costs of which many users are likely unaware, including violations to one's right to autonomy, privacy, non-discrimination, freedom of expression, and consumer protection.

The terms of service (ToS) and privacy policy agreements (PPA) of these apps supposedly provide users with the information they need to weigh the costs and benefits of using the app and provide their informed consent to the terms and practices that are specified in them. However, ToS and PPA—the main tools used to define the legal relationship between users and mobile app providers—are generally long, complex, and difficult to understand. Furthermore, due to the prevalence of mobile apps, users are asked to sign many ToS and PPA. For these reasons, users tend to automatically sign these documents without reading them—i.e., without providing their *informed* consent to the terms. This practice is problematic because ToS and PPA are legally binding documents that may include unethical provisions that users do not reasonably expect.<sup>1</sup> This Article refers to these issues as “ethical risks.”

This Article presents a novel typology of the ethical risks that are hidden within ToS and PPA. Based on this thorough analysis, the Article argues that the legal mechanisms of ToS and PPA do not achieve their purposes. ToS and PPA often legalize ethical risks by obtaining users' consent to terms that they may not fully understand. As such, rather than protecting users, ToS and PPA frequently perpetuate users' vulnerabilities and subject them to rights-infringing measures.

To construct a novel comprehensive typology of ethical risks, this Article employs a methodology of qualitative thematic analysis. This included an extensive qualitative review of numerous sources from the fields of digital apps, big data, and data analysis, including academic publications, reports of privacy agencies, consumer protection agencies and non-government organizations (NGOs), various regulations, and other governmental and legislative papers.

The proposed typology provides a conceptual framework for considering ethical risks in ToS and PPA. It offers several novel contributions; previous studies that dealt with risks in PPA of digital apps are limited in that they narrowly address only privacy violations rather than a more com-

---

1. See Cheryl B. Preston & Eli W. McCann, *Unwrapping Shrinkwraps, Clickwraps, and Browsewraps: How the Law Went Wrong from Horse Traders to the Law of the Horse*, *BYU J. OF PUB. L.* 26, 18–19, 22–23 (2012); Florencia Marotta-Wurgler, *Some Realities of Online Contracting*, 19 *SUP. CT. ECON. REV.* 11–13 (2011); Florencia Marotta-Wurgler & Daniel L. Chen, *Does Contract Disclosure Matter?*, 168 *J. INSTITUTIONAL & THEORETICAL ECON.* 94, 95–97 (2012).

prehensive framework of ethical risks.<sup>2</sup> In addition, previous empirical studies aimed at uncovering ethical risks in PPA are based on a risk typology developed by computer scientists rather than by legal domain experts.<sup>3</sup> Moreover, by examining ethical risks in both ToS and PPA, the proposed typology in this research addresses ethical risks that go beyond privacy violations, discussing user vulnerability with respect to an expanded set of rights, including the rights to autonomy, non-discrimination, freedom of expression, and consumer protection. This broader conceptualization of ethical risks in PPA and ToS of mobile apps is necessary for the development of a comprehensive policy solution that could address the multitude of problems that they pose.

The proposed typology can be effectively applied across a multitude of fields and for a variety of purposes. First and foremost, the typology is intended to improve the accessibility and comprehensibility of ethical risks in ToS and PPA. Therefore, the typology can be used to educate users and help them make informed decisions regarding the apps they choose to use and the manner in which they use them. The typology and analysis may also help mobile app providers draft more ethical ToS and PPA. Furthermore, the findings may prompt privacy protection and consumer protection regulators to broaden the scope of their regulation and enforcement activities and to reconsider the regulatory requirements in this domain (thus mitigating the identified ethical risks to users). Moreover, the typology forms a useful baseline for empirical studies that address user perceptions of ethical risks, as well as for studies that seek to analyze the contents of PPA and ToS. Specifically, it can serve as the basis for the work of computer scientists who develop automated tools to identify ethical risks in apps.

This Article includes four parts: Part I explains the terms ToS and PPA and raises the question of whether they are the right tools to protect user rights, in particular users' right to autonomy. Part II reviews the concept of ethical risks in mobile apps and divides the different risks into three categories: (1) ethical risks arising from the content of ToS and PPA; (2) ethical risks that stem from users' lack of informed decision-making regarding ToS and PPA; and (3) ethical risks external to ToS and PPA. Part III explores and explicates the first category of risks and presents a typology of ethical risks arising from the content of ToS and PPA and how these risks violate user autonomy. Additionally, it examines how the four key laws in the area of digital privacy and consumer protection—the General Data Protection Regulation (GDPR), the Consumer Rights Directive

---

2. See Vinayshekhar Bannihatti Kumar et al., *Quantifying the Effect of In-Domain Distributed Word Representations: A Study of Privacy Policies*, in AAAI SPRING SYMPOSIUM ON PRIVACY-ENHANCING ARTIFICIAL INTELLIGENCE AND LANGUAGE TECHNOLOGIES 46 (2019); Welderufael B. Tesfay et al., *I Read but Don't Agree: Privacy Policy Benchmarking Using Machine Learning and the EU GDPR*, in COMPANION PROCEEDINGS OF THE WEB CONFERENCE 163 (2018).

3. *Supra* note 2.

of the European Union (EU), the California Consumer Privacy Act (CCPA), and the California Privacy Rights Act (CPRA)—protect (or fail to protect) against the ethical risks identified in the typology. Part IV discusses the typology's potential applications.

#### I. FRIEND OR FOE? MOBILE APP AGREEMENTS AS REGULATORY MECHANISMS FOR PROTECTING USERS' AUTONOMY

In recent years, an acceleration in technological developments has affected virtually every area of our lives and changed the way we interact, work, and think. Many of these changes are positive and have upgraded our quality of life.<sup>4</sup> For example, the various social apps (e.g., Facebook, Instagram, and TikTok) provide people with access to information and the ability to connect with family and friends easily, quickly, and comfortably.<sup>5</sup> Some apps also target specific audiences by offering personalized products, and thus, the search for relevant products becomes simpler and more accessible.<sup>6</sup> These changes have also allowed for more efficient advertising, connecting businesses with consumers who want to purchase their products and services. Further, technology has created healthy competition, which encourages consumers to compare prices and thus requires suppliers to lower prices and adjust to market prices. At the click of a button, customers can find a desired product or service at the best price and desired level of quality.<sup>7</sup> Nowadays, almost any service, including making a doctor's appointment, requesting a passport extension, retrieving medical documents, filing court documents, and more, can be performed from the comfort of one's home.<sup>8</sup> Such changes and technological developments have led to the increased use of mobile devices and digital apps, and consequently, to the signing of many ToS and PPA that define the legal relationship between users and mobile app providers.

ToS are adhesion contracts that govern the legal relationship between digital apps and their users. Users must accept ToS in order to use the offered service.<sup>9</sup> ToS typically contain sections pertaining to some, or all,

4. See Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 64–65 (2012).

5. See Gil Appel et al., *The Future of Social Media in Marketing*, 48 J. ACAD. MARKETING SCI. 79, 79, 84 (2019).

6. See Avita Katal et al., *Big Data: Issues, Challenges, Tools and Good Practices*, in 2013 SIXTH INTERNATIONAL CONFERENCE ON CONTEMPORARY COMPUTING (IC3) 404 (2013).

7. See Kiran Baktha et al., *Social Network Analysis in Healthcare*, in INTERNET OF THINGS AND BIG DATA TECHNOLOGIES FOR NEXT GENERATION HEALTHCARE 309 (Chintan Bhatt et al. eds., 2017).

8. See Charith Perera et al., *Big Data Privacy in the Internet of Things Era*, 17 IT PROF. 32 (2015).

9. See AOL *Dumps New Member Policy*, CNET (July 29, 1997), <https://www.cnet.com/news/aol-dumps-new-member-policy/> [https://perma.cc/8MEA-N9FK].



of the following topics: definition of keywords and phrases; user rights and responsibilities; users' and providers' accountability for online actions, behavior, and conduct; payment details such as membership or subscription fees; a dispute resolution clause detailing the dispute resolution process, which typically includes arbitration, and oftentimes the limited rights of users to take a claim to court; disclaimers and limitations of liability, which clarify the providers' legal liability for damages incurred by users; and other topics that will be discussed extensively in the typology Section.<sup>10</sup>

PPA are statements or legal documents that disclose some or all of the ways a party gathers, uses, discloses, and manages customer data.<sup>11</sup> Within PPA, the app provider discloses to the customer what specific information will be collected, whether the information will be confidential or transferred to third parties, for what purpose the information will be used, how the information can be deleted or changed, what processing is done to the information, etc.<sup>12</sup> The exact contents of any particular PPA depend upon the applicable laws and may need to address different requirements across geographical boundaries and legal jurisdictions.<sup>13</sup>

ToS and PPA, each within the scope of their responsibilities, are supposed to protect the rights of users and provide them with tools to provide "informed consent"<sup>14</sup> when they consider the costs and benefits of using the app. The meaning of informed consent in the context of privacy law, and in standard contracts and consumer protection contexts, is that the object of information has the necessary information to decide whether to consent to the provision of information and its uses, including the transfer of information to third parties.<sup>15</sup> Building on the work of sociologist Alan

10. See Florencia Marotta-Wurgler & Robert Taylor, *Set in Stone? Change and Innovation in Consumer Standard-Form Contracts*, 88 N.Y.U. L. REV. 240 (2013).

11. This Article proceeds from the premise that PPA, similar to ToS, are considered binding legal contracts. However, from a legal perspective, there is no clear consensus around PPA as legally binding contracts. See Oren Bar-Gill et al., *Searching for the Common Law: The Quantitative Approach of the Restatement of Consumer Contracts*, 84 U. CHI. L. REV. 7, 28–30 (2017); Scott Killingsworth, *Minding Your Own Business: Privacy Policies in Principle and in Practice*, 7 J. INTELL. PROP. L. 57, 91–92 (1999).

12. See Kumar et al., *supra* note 2, at 1; Joel R. Reidenberg et al., *Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards*, 96 WASH. U. L. REV. 1409, 1412–13 (2019).

13. See ANN CAVOUKIAN & DON TAPSCOTT, WHO KNOWS: SAFEGUARDING YOUR PRIVACY IN A NETWORKED WORLD 97 (1997).

14. The term "informed consent" is derived from the medical world. The term has been defined as a "procedure for ensuring that research subjects understand what is being done to them, the limits to their participation and awareness of any potential risks they incur." SOCIAL RESEARCH ASSOCIATION, ETHICAL GUIDELINES 28 (2003).

15. See Commission Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter GDPR]. Article 4(11) refers to consent that is "specific, informed and unambiguous." *Id.* at 34. Section 7 of the GDPR provides further instructions about consent. *Id.* at 37.

Westin, Michael D. Birnhack interprets the phrase “informed consent” as individuals’ ability to exercise control over their autonomous unit.<sup>16</sup> This ability is only possible when people understand the meaning of the requested action. In other words, the ability for consent occurs when individuals realize that information about them will be collected, agree to the collection of information, and agree to the various uses of that information. Consent is the core of users’ abilities to protect themselves from possible infringements of their rights. It allows users the freedom of choice and control to decide whether and how to use a particular app.

As mentioned, ToS and PPA are the primary means of obtaining informed consent from individuals. Thus, the way in which ToS and PPA are implemented becomes an important regulatory mechanism for protecting users’ rights. These agreements should clearly reveal to users all the information needed to make an informed decision regarding whether and how to use any particular app.<sup>17</sup>

However, ToS and PPA are lengthy and complex, making it almost impossible for typical users to fully understand what they are agreeing to when they sign these documents.<sup>18</sup> In essence, this lack of understanding creates a situation of uninformed consent and unethical usage of user data, otherwise known as “ethical risks.” As will be described in further detail in the following sections, the different ethical risks can be divided into three groups:

(1) *Ethical risks arising from the content of ToS and PPA.* This group of risks is the focus of Part III and includes seven primary risks. These seven risks are: uninformed consent, restricting user legal action, limited readability, profiling, processing user information, tracking user information, and third-party data transfers. The seven primary risks are comprised of multiple secondary risks, which will be presented in detail in the typology Section.

(2) *Ethical risks that stem from users’ lack of informed decision-making regarding ToS and PPA.* This group of risks focuses on human behavior and the way that app users perceive ToS and PPA. Among the risks that will be presented are the tendency of users not to read ToS and PPA and not to attribute adequate weight to the cost of privacy violations.

(3) *Ethical risks that are external to ToS and PPA.* This group of risks includes risks that users cannot identify in ToS or PPA because they are external to the service relationship of the app provider and the user. Among the risks that will be presented are information security failures and identity theft.

---

16. Michael D. Birnhack, *Control and Consent: The Theoretical Basis of the Right to Privacy*, 11 L. & GOV'T IN ISRAEL 9, 41–42 (2007) (Isr.) (Hebrew).

17. See Omri Ben-Shahar & Lior Jacob Strahilevitz, *Contracting Over Privacy: Introduction*, 45 J. LEGAL STUD. S1, S1–S6 (2016).

18. See Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303, 312–14 (2008); Marotta-Wurgler & Chen, *supra* note 1, at 96, 110.

These three groups of risks lead to many violations of user rights. One of the biggest violations is the violation of individual autonomy. Autonomy refers to individuals' abilities to make meaningful decisions about their own lives and behaviors without external intervention. People have desires and intentions and often act based on these intentions to choose the right path for themselves. They can choose how they want to manage their lives, for example religiously or secularly, whom they want to marry, where they want to work, for whom they want to vote, and more.<sup>19</sup> As Joseph Raz describes, "[t]he ruling idea behind the ideal of personal autonomy is that people should make their own lives."<sup>20</sup> This broad understanding of individual autonomy gives rise to many other rights, such as the right to freedom of expression, the right to equality, the right to religion and religious freedom, the right to privacy, and more.<sup>21</sup>

From the above description of autonomy, one can conclude that control is the key to realizing one's autonomy. In today's world, one way to protect individuals' autonomy rights and to give them responsibility over their destiny and decisions is to allow them to control the use of their information. In regard to apps, this means that individuals should have the right to choose with which apps they want to share their information, but only after being aware of the various risks that exist. This knowledge will allow them to make an informed choice of whether they are willing to accept the risks involved in using the app. However, if users do not understand the various risks, they will not be able to make an informed decision regarding their agreement to them. Because the various ethical risks are hidden within ToS and PPA, an absurd situation is created: instead of being a tool that protects users from the risks of using digital apps, ToS and PPA have become tools that legalize all app providers' actions, even those that are considered unethical, because the users have allegedly consented to them.<sup>22</sup>

This Article presents the various risks that arise from the use of mobile apps. It begins by presenting all the risks and then focusing on the risks that are hidden within ToS and PPA. It also examines how the various risks create violations of user autonomy, explains why the existing ToS and PPA tools are not sufficient, and provides suggestions for change. As part of the presentation of the risks that are hidden within ToS and PPA, the Article also examines whether consumer protection and privacy protection legislation in the U.S. and Europe addresses these risks, because mobile app users are likely to expect to find information about their rights

---

19. Daniel Susser et al., *Technology, Autonomy, and Manipulation*, 8 INTERNET POL'Y REV., June 30, 2019, at 1, 8–9.

20. JOSEPH RAZ, *THE MORALITY OF FREEDOM* 369 (1986).

21. See Bart van der Sloot & Sascha van Schendel, Article, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, 7 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 110, 117, 119, 126 (2016).

22. See MICHAEL D. BIRNHACK, *PRIVATE SPACE: THE RIGHT TO PRIVACY, LAW AND TECHNOLOGY* 99–106 (2010) (Isr.) (Hebrew).

in the key legislative instruments in these domains. To this effect, the Article focuses on four regulation schemes, which represent the state of the art in these domains:

(1) *The European General Data Protection Regulation (GDPR)*. The GDPR is a compilation of mandatory provisions adopted by the European Parliament, the Council of the European Union, and the European Commission to regulate information issues in European Union (EU) territory.<sup>23</sup> The regulation applies to the collection, retention, and transfer of private individuals' personal data and establishes uniform rules for the protection of privacy. The GDPR is the most up-to-date and comprehensive regulatory development in information policy. It is important to note that, although the GDPR is a significant law that has drawn praise and been implemented worldwide, one of its drawbacks is that the law does not address all consumer domains. Rather, it focuses only on data protection in the private domain. The lack of consumer protection is a significant part of the risks that are reflected in ToS and, therefore, it is important to address this particular risk as well. Thus, this Article's account of ethical risks as they relate to European legislation refers to both the GDPR and the Consumer Rights Directive of the EU, which will be explained next.

(2) *The Consumer Rights Directive of the EU*. This directive aligns and harmonizes national consumer rules. For example, the directive defines the information that consumers need to be given before they purchase a product, and states that consumers have the right to cancel online purchases in the EU. Recently, the directive has been amended by EU Directive 2019/2161 of November 27, 2019, which increased the enforcement of consumer protection laws.<sup>24</sup>

(3) *The California Consumer Privacy Act (CCPA)*. California became the first U.S. state with a comprehensive consumer privacy law when it enacted the CCPA of 2018.<sup>25</sup> This Act increases the scope of California residents' rights over their personal data and addresses the responsibilities of organizations in regard to data protection. The law was enacted on January 1, 2020, but enforcement of the law began on July 1, 2020. The law addresses both consumer and privacy aspects.

(4) *The California Privacy Rights Act (CPRA)*. On November 3, 2020, California voters approved Proposition 24 (the CPRA).<sup>26</sup> The CPRA amends key portions of the CCPA. The CPRA gives additional rights to consumers and places additional obligations on businesses. The new law provides additional protections for sensitive personal information, ex-

23. See GDPR, *supra* note 15.

24. Directive 2011/83/EU, of the European Parliament and of the Council of 25 October 2011 on Consumer Rights, Amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and Repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council, 2011 O.J. (L 304) 1.

25. See Cal. Civ. Code §§ 1798.100-1798.199 (West 2020).

26. See S. 746, 2021 Leg., Reg. Sess. (Cal. 2021).

pands CCPA's opt-out rights to include new types of information sharing, and requires businesses to provide additional mechanisms for individuals to access, correct, or delete data, with a particular focus on information used by automated decision-making systems. The CPRA is scheduled to become operative in 2023. This Article addresses this law though it has not yet been implemented, as it complements the CCPA in many aspects of information protection and addresses ethical risks that the CCPA has not addressed. Referring to the two laws together will make it possible to obtain a complete picture of consumer protection and privacy protection in California.

## II. ETHICAL RISKS OF MOBILE APPS

This Part introduces the concept of ethical risks in mobile apps and divides risks into categories. Ethical risks in ToS and PPA refer to practices or arrangements that are not considered illegal per se but may nonetheless be inappropriate, lead individuals to feel a sense of discomfort, or result in considerable harm to users. In other words, ethical risks may be viewed as the "grey area" of ToS and PPA. As such, they are more difficult to detect and manage than strictly illegal practices.

The ethical risks in digital apps are manifold; however, this Article divides them into three conceptual risk types:

- (1) ethical risks arising from the content of ToS and PPA;
- (2) ethical risks that stem from users' lack of informed decision-making regarding ToS and PPA; and
- (3) ethical risks that are external to ToS and PPA.

This Article focuses on the first category, which will be explained in detail in Part III. The two other risk categories pertain to risks that are external to the content of PPA and ToS. In this Section, the Article will briefly introduce the three conceptual risk types, provide examples of risks from each group, and explain how the various risks harm users' autonomy.

### A. *Ethical Risks Arising from the Content of ToS and PPA*

This group of risks includes all the risks that are explicitly listed in ToS and PPA of apps. Almost every app provider requests that users confirm they have read and understood PPA and agree to ToS. Users must sign these documents by marking that they have read the statement before being able to use the app. The risks that the app providers specify in their agreements may thus become legal since users have allegedly agreed to them.

This group of risks may be the most important to acknowledge because, unlike the other two groups, the risks are controllable by both the users and the app providers. If users were exposed to the various risks that accompany the use of an app through a new type of data protection frame-

work, such as a discovery document that would be accessible and easy to read, they would be given the opportunity to make an informed decision on whether to use the app. Also, if users' knowledge of the existence of the risks affects them and prevents them from using apps, app providers may have an incentive to reduce risks by engaging in genuine risk management.

Due to the great importance of this group of risks, the Article focuses on identifying and creating a typology of them. Therefore, all the risks associated with this category will be discussed extensively in Part III.

B. *Ethical Risks That Stem from Users' Lack of Informed Decision-Making Regarding ToS and PPA*

One of the major risks that exists in ToS and PPA of digital apps is the way people treat these agreements. Most app users view the agreements as an obstacle to get past on the way to using the app. They do not read the agreements and even if they did read them, it would not necessarily affect their decision about whether or not to use the app. Additionally, many users misunderstand the context of ToS and PPA. Further, when users choose whether to accept or reject ToS and PPA that violate their privacy, they act in accordance with bounded rationality principles.<sup>27</sup> People have a set of considerations when choosing whether to use an app and the content of the agreements and the risks they include therein are not necessarily within the bounds of users' considerations.<sup>28</sup> For example, if all the user's friends use an app, they may choose to use it even if the agreements specify many risks.

This Article proposes to subdivide the group of risks into several secondary risks as presented below:

1. *The Term "Privacy Policy" Misleads Users Into Thinking That Their Privacy Is Protected*

Due to a lack of knowledge regarding the legal significance of PPA, some users mistakenly believe that the very existence of such a document means that the app providers will protect their privacy. "Thus, it is not surprising that the mere presence" of PPA "inclines [users] to disclose more personal information."<sup>29</sup> Alarming, a 2014 survey of American internet users found that forty-four percent of the individuals surveyed be-

---

27. There is significant scholarship regarding the definition of "bounded rationality." John Conlisk, *Why Bounded Rationality?*, 34 J. ECON. LITERATURE 669 (1996); James G. March, *Bounded Rationality, Ambiguity, and the Engineering of Choice*, 9 BELL J. ECON. 587 (1978); Bertrand Munier et al., *Bounded Rationality Modeling*, 10 MARKETING LETTERS 233 (1999); Reinhard Selten, *Bounded Rationality*, 146 J. INSTITUTIONAL & THEORETICAL ECON. 649 (1990).

28. See Idris Adjerid et al., *A Query-Theory Perspective of Privacy Decision Making*, 45 J. LEGAL STUD. S97, S99-S100 (2016).

29. RENÉ ARNOLD ET AL., PERSONAL DATA AND PRIVACY 3 (2015).

lieved that the mere posting of a PPA meant that personal data collected by the company would not be disclosed.<sup>30</sup>

### 2. *Users Do Not Read the Terms of Service and Privacy Policy Agreements*

Because ToS and PPA of apps are usually difficult and cumbersome to read, users rarely read them. This behavior appears to be common both when signing up for new services and when changes are made to PPA and ToS for services that individuals are already using. For example, one study of 543 users found that seventy-four percent of participants accepted ToS and PPA without reading them at all. Of the participants who chose to read ToS and PPA, the majority spent very little time reading and largely skipped through the text and clicked “accept.” The average time spent on reading both PPA and ToS was about fourteen seconds, a length of time that is clearly insufficient to allow for informed consent or to be considered as reading the text at all.<sup>31</sup>

Another study conducted by the British Communications Authority (Ofcom), published in May 2015, found that users tended to approve ToS without reading them and that, even when users accessed ToS, they usually did not read them (the average time viewing ToS was under one minute).<sup>32</sup> In addition, another study found that only one or two of every 1,000 software shoppers accessed the license agreements and that most of those who accessed the agreements read only a small portion.<sup>33</sup> Because users do not read ToS and PPA of digital apps, they are not aware of the risks inherent in them, leading to a major violation of users’ autonomy and other rights. Therefore, users’ consent to these agreements is not free and informed.

### 3. *Users Do Not Attribute Adequate Weight to the Cost of Privacy Violations*

Various studies show that when users perceive many benefits to sharing their information with a particular service—e.g., technological advantages, decreased feelings of loneliness, social connection, lifestyle improvement—their concern about privacy violations diminishes. In other words, the more benefits that users perceive from using an app, the less they will view the app as posing a danger to them.<sup>34</sup> When users choose whether to approve or disapprove ToS and PPA that violate their

30. See Aaron Smith, *What Internet Users Know About Technology and the Web*, PEW RES. CTR. (Nov. 25, 2014), <https://www.pewresearch.org/internet/2014/11/25/web-iq/> [<https://perma.cc/LK7C-BYY4>].

31. See Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO. COMM. & SOC’Y. 128, 141 (2018).

32. See RENÉ ET AL., *supra* note 29, at 2.

33. See Yannis Bakos et al., *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 3 (2014).

34. See Jaspreet Bhatia, *Ambiguity in Privacy Policies and Perceived Privacy Risk* (Apr. 19, 2019) (unpublished Ph.D. thesis, Carnegie Mellon University) (on file with Carnegie Mellon University).

privacy protections, they are likely to follow the principles of bounded rationality. The process that users go through to decide whether to approve ToS and PPA is a process that does not regard the cost of disclosing one's personal information. Users tend to only look at the benefits of using an app and disregard costs altogether.<sup>35</sup>

### C. *Ethical Risks That Are External to ToS and PPA*

This group of risks includes risks that users cannot identify in ToS or PPA because they are external to the service relationship between the app provider and the user. These risks are associated with user data that are gleaned from the app by third parties and used for purposes outside the scope of the service(s) provided through the app. This type of information transfer usually results from data security breaches from either within the app or from other companies with which the app works.<sup>36</sup> This group of risks also addresses the possible implications of disclosing and misusing user information to manipulate users.

The ethical risks of this group can be subdivided into several secondary risks as presented below:

#### 1. *Information Security Failures*

The smartphone user environment is based on a significant number of service providers across several commercial layers of the product, including the company that manufactures the mobile phone, the company that develops the operating system of the device, the media companies that operate the product, the app stores, the app developers, the content providers, online services, and various third parties (e.g., advertiser networks).<sup>37</sup> The vast amount of user information that is collected across the internet, along with the number of actors involved in the information collection, processing, storage, usage, and more, creates great concern for security breaches of personal information.<sup>38</sup> If a problem arises in even one area in the chain of players, the potential for a data breach by third parties is heightened.<sup>39</sup> In the current era, in which many operations take place behind computer screens—as opposed to face-to-face interactions—

35. See Adjerid et al., *supra* note 28, at S114–S115.

36. See Tehilla Shwartz Altshuler, INTRODUCTION TO PRIVACY IN AN ERA OF CHANGE 11–15 (Isr. Democracy Inst. 2012) (Isr.) (Hebrew).

37. See Article 29 Data Prot. Working Party, Opinion 02/2013 on Apps on Smart Devices, 00461/13/EN, WP 202, at 2 (Feb. 27, 2013).

38. *Id.* at 5.

39. See Katharine Kemp, *Concealed Data Practices and Competition Law: Why Privacy Matters*, 16 EUR. COMPETITION J. 628, 644–45 (2020). Examples of security breaches can be found in a 2016 report by the Israeli Registrar of Databases. In one incident, a backup drive of a statistical database of a car insurance company was stolen. In another, information on candidates for a Haifa military boarding school was leaked due to a breach in the Haifa Military Board's website. A link to a data file containing sensitive personal information of applicants was found and uploaded to the Internet. The boarding school was found to have failed to fulfill



users have difficulty tracking the location of the information collected about them and controlling the quality of protection regarding their personal information.<sup>40</sup> A related risk concerns the commercializing of user information by companies or entities that sell information to third parties.<sup>41</sup> In Israel, the Privacy Authority has investigated numerous cases of information trading.<sup>42</sup>

## 2. *Identity Theft*

One of the major concerns in the era of big data is identity theft. Identity theft occurs when someone seeks to take over a person's identity in various ways, such as stealing credit card details, using the person's name to commit a criminal offense, and more. Often, in cases of identity theft, it takes a long time for the persons whose identities have been stolen to discover the theft; even after the identity theft is discovered, it takes a long time to repair the damage (clearing one's name in the case of a criminal offense, recovering lost money in the case of credit card theft, repairing one's damaged reputation, etc.). This difficulty is exacerbated in the case of biometric identity theft, a situation in which a person's physical features—their iris scans or fingerprints—are stolen from digital databases and used to impersonate them.<sup>43</sup>

## 3. *Online Manipulation Based on Collected (and Transferred) Data*

Manipulation of individuals involves an attempt to influence them and change their decision-making process covertly and deliberately. Targeted advertising based on users' profiles is meant to manipulate and influence users' choices and the reasons for choosing a particular option.<sup>44</sup> Companies combine insights from the fields of psychology, neuroscience, and behavioral economics with new digital technologies and social media, to move beyond simply measuring customer behavior to designing and creating products with the specific goal of forming new habits.<sup>45</sup> In recent years, political campaigns have begun to utilize this

---

the duty of information security stipulated in section 17 of the Privacy Protection Law, 1981, due to not having any control or monitoring systems in place.

40. See Altshuler, *supra* note 36; Birnhack, *supra* note 22.

41. See Amir Fuchs, *Terrorism and Privacy—A Proposal for Rethinking the Tools for Coping with Terrorism Online*, in *PRIVACY IN AN ERA OF CHANGE* 231, 242–43 (Tehilla Schwartz Altshuler ed., 2012) (Isr.) (Hebrew).

42. For example, a 2016 investigation by the Privacy Protection Authority in Israel regarding the trade of medical information revealed that nursing companies bought medical information of elderly hospital patients to conduct targeted patient marketing. For more information about the investigation, see Report of the Registrar of Databases for 2016, at 16 (published in August 2017).

43. See Kemp, *supra* note 39, at 646.

44. See Susser et al., *supra* note 19, at 9.

45. See Nanette Byrnes, *Technology and Persuasion*, *MIT TECH. REV.* (Mar. 23, 2015), <https://www.technologyreview.com/s/535826/technology-and-persuasion/> [<https://perma.cc/JE63-PGT7>].

tactic by implementing sophisticated algorithms and modeling techniques to infer voters' preferences, intentions, and beliefs, link personal characteristics with political beliefs, and specifically target undecided voters.<sup>46</sup> Such techniques affect the core of the democratic process, compromising values that are necessary preconditions for democratic life, such as political privacy.<sup>47</sup>

When these tactics are employed, personal information can be analyzed and used to affect individuals' conduct and the choices they make.<sup>48</sup> For example, in the 2016 U.S. election campaign, Facebook admitted that 150 million Americans watched advertisements that were sponsored by Russia. This was made possible by Facebook's algorithm, which is designed to "maximize engagement[.]"<sup>49</sup> This manipulative action undermines individual autonomy in two ways: (1) causing an individual to act in ways they did not intend; and (2) causing an individual to act for reasons they did not intend.<sup>50</sup>

In the following section, the Article will present a typology of the ethical risks that arise from the content of ToS and PPA.

### III. NOVEL TYPOLOGY OF ETHICAL RISKS ARISING FROM THE CONTENT OF TO S AND PPA

In this Part, the Article identifies the ethical risks in the text of ToS and PPA through a thematic analysis of the literature in this domain, as detailed below. Based on the analysis, the Article proposes a new typology by classifying these risks in distinct categories.

#### A. Methodology

The research question that guided the current study was: "What are the ethical risks that exist in ToS and PPA of digital apps?" To answer this question, I conducted a qualitative review spanning 178 sources that address the risks involved in using digital apps, as well as the risks of big data and data analysis. Sources included academic publications, reports conducted by privacy agencies and consumer protection agencies, as well as by various NGOs, regulations, and governmental and legislative papers. I identified sources from legal databases and the internet based on the keywords "ethical risks" and "digital apps." I extracted themes from sources that were relevant to the topic.

46. See Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 882 (2014).

47. See Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426–28 (2000).

48. See Susser et al., *supra* note 19, at 2–3, 6.

49. Jonathan Freedland, *From Peppa Pig to Trump, the Web Is Shaping Us. It's Time We Fought Back*, GUARDIAN (Nov. 17, 2017), <https://www.theguardian.com/commentisfree/2017/nov/17/peppa-pig-donald-trump-internet-social-media-algorithms> [<https://perma.cc/9Z4W-DVEM>].

50. See Susser et al., *supra* note 19, at 1–2.

To analyze the source text, I employed the widely used process of thematic analysis that was developed by Virginia Braun and Victoria Clarke.<sup>51</sup> In accordance with this process, after familiarizing oneself with the various sources, the researcher highlights the topics relevant to the research question (i.e., related to ethical risks). Next, the researcher codes topics into themes and consolidates sets of themes in a table, where they indicate item names and quotes from the data that exemplify individual themes.

After completing the table of themes, I examined the table to create a model summarizing all the different ethical risks. I compared and combined similar risks, and when I identified a relatively limited number of risks, I examined and categorized relationships between them as either primary risks or secondary risks. In the end, I identified seven primary risk categories and used them to create the typology of ethical risks arising from the content of ToS and PPA.

#### B. *Analysis and Results: The Ethical Risks Typology*

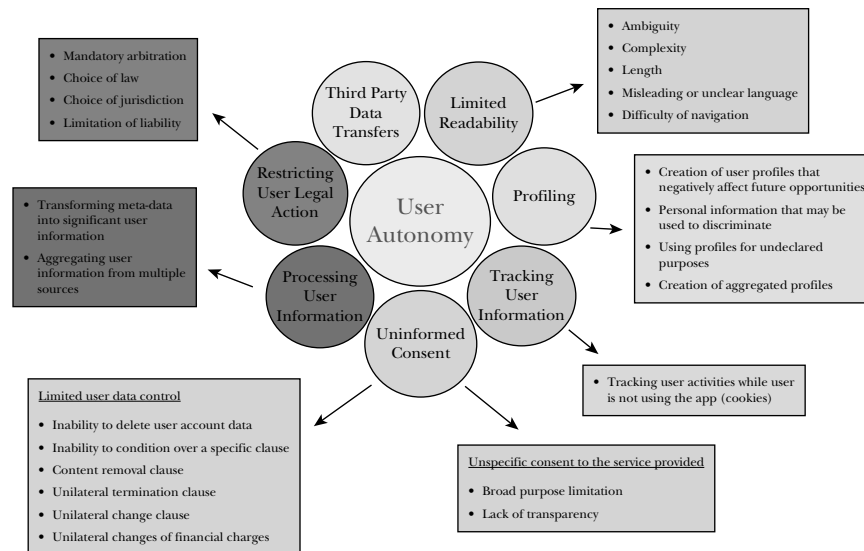
This Section presents the ethical risks that are typically included in standard ToS and PPA. These are classified into seven primary risks, each of which includes several secondary risks. Figure 1 graphically represents these risks. Additionally, the Article examines four central laws related to ethical risks identified in this typology—the GDPR, the Consumer Rights Directive of the EU, the CCPA, and the CPRA.

The various risks are interrelated, and therefore, some secondary risks cross the bounds of several primary risks. Nevertheless, the separate classifications were maintained to facilitate lay readers' understanding and create a clearer and simpler typology that is practical and can be implemented effectively.

---

51. Virginia Braun & Victoria Clarke, *Thematic Analysis*, in 2 APA HANDBOOK OF RESEARCH METHODS IN PSYCHOLOGY 57 (Harris Cooper et al. eds., 2012); Victoria Clarke & Virginia Braun, *Thematic Analysis*, 12 J. POSITIVE PSYCHOL. 297 (2017); see also Deborah Anderson et al., *Reviewing the Literature Using the Thematic Analysis Grid*, in PROCEEDINGS OF THE 14TH EUROPEAN CONFERENCE ON RESEARCH METHODOLOGY FOR BUSINESS AND MANAGEMENT STUDIES 455; Cecily Young et al., *Hindering Resilience in the Transition to Parenthood: A Thematic Analysis of Parents' Perspectives*, J. REPROD. & INFANT PSYCHOL., May 22, 2020.

FIGURE 1: ETHICAL RISKS ARISING FROM THE CONTENT OF TOS AND PPA



According to the results of the research, the various risks can be divided into seven primary risks:

### 1. *Uninformed Consent*

In the face of significant potential for violations of user rights, ToS and PPA are the principal means for obtaining users' consent to the utilization of their personal information. However, the attributes of ToS and PPA create heightened ethical risks that cast doubts on users' ability to grant their informed consent for personal data use.<sup>52</sup> App providers require users to consent to ToS and PPA to use apps, but because the agreements are full of hidden risks, of which users are either unaware or to which they do not attach sufficient importance, the users' consent is simply a rubber stamp of approval rather than true, free, and informed consent.<sup>53</sup>

The meaning of informed consent is that the object of information has the necessary knowledge to decide whether to consent to the provision of information and its processing, including its transfer to third parties.<sup>54</sup> This interpretation corresponds to the definition of the term "informed consent" in Article 4 of the GDPR, such that in order for users to provide informed consent, the app provider must provide users with details regarding the use of their personal information.<sup>55</sup> Such details would in-

52. See Marotta-Wurgler, *supra* note 1, at 22.

53. See Daniel Nunan & Baskin Yenicioğlu, *Informed, Uninformed and Participative Consent in Social Media Research*, 55 INT'L J. MKT. RES. 791 (2013).

54. See Birnhack, *supra* note 16, at 100.

55. See GDPR, *supra* note 15, Article 4.

clude a description of information that will be collected and stored, the purposes for which the information will be processed, the type of information to be processed, and the risks that arise from data transfer. Consent must be unequivocal and objective; it cannot be implied.<sup>56</sup>

The informed consent risk has earned senior status and broad protection under the GDPR, a law which regards consent as one of the core elements of privacy protection. As such, the GDPR addresses the matter of consent across a number of the articles of the law. The basic requirements for valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR.<sup>57</sup> Consent must be freely given, voluntary, specific, informed, and unambiguous. In addition, there are many other sections in the GDPR that refer to consent.<sup>58</sup> In the CCPA, unlike the GDPR, there is no specific reference to informed consent. Rather, the reference to informed consent is indirect across different sections.<sup>59</sup>

The CPRA extends the reference given to the term consent in the CCPA. Section 1798.140, the definitions section, describes the term consent as “any freely given, specific, informed, and unambiguous indication of the consumer’s wishes by . . . a statement or by a clear affirmative action, signify[ing] agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.”<sup>60</sup> The section states that:

[a]cceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent. Hovering over, muting, pausing, or closing a given piece of content does not constitute consent. Likewise, agree-

---

56. See GDPR, *supra* note 15, recital 32.

57. See *id.*, Article 7 and recital 32.

58. See *id. passim*. The relevant GDPR articles are: (Art. 4 GDPR) Definitions; (Art. 6 GDPR) Lawfulness of processing; (Art. 7 GDPR) Conditions for consent; (Art. 8 GDPR) Conditions applicable to child’s consent in relation to information society services; (Art. 9 GDPR) Processing of special categories of personal data; (Art. 22 GDPR) Automated individual decision-making, including profiling; (Art. 49 GDPR) Derogations for specific situations. *Id.* The relevant Recitals are: (32) Conditions for Consent; (33) Consent to Certain Areas of Scientific Research; (38) Special Protection of Children’s Personal Data; (40) Lawfulness of Data Processing; (42) Burden of Proof and Requirements for Consent; (43) Freely Given Consent; (50) Further Processing of Personal Data; (51) Protecting Sensitive Personal Data; (54) Processing of Sensitive Data in Public Health Sector; (71) Profiling; (111) Exceptions for Certain Cases of International Transfers; (155) Processing in the Employment Context; (161) Consenting to the Participation in Clinical Trials; (171) Repeal of Directive 95/46/EC and Transitional Provisions. *Id.*

59. For example, section 1798.105 states that if users have agreed to their information not being deleted, it can remain in the system. Another example is section 1798.120, which deals with transferring information to third parties and states that user consent is required to transfer the information. See CAL. CIV. CODE §§ 1798.105, 1798.120 (West 2020).

60. *Id.* § 1798.140.

ment obtained through use of dark patterns does not constitute consent.<sup>61</sup>

From the section it is clear that the consent should be specific and unequivocal regarding a document that is clearly written to the reader. The overall risk of users not granting their free and informed consent can be classified into two distinct primary risks.

a. Unspecific Consent to the Service Provided

ToS and PPA require users to confirm that they have read the terms and that they specifically understand and agree to them. However, such a request poses a risk because users cannot give specific consent to the services provided. This inability to provide specific consent results from the following secondary risks:

i. Broad Purpose Limitation

The bargaining power of app providers frequently enables them to obtain consent from users for a broad range of conduct. By bundling consent to multiple and separate practices, digital platform providers push users to enter into contracts without allowing them to choose which data collections, uses, and disclosures they agree to and which they do not. As a result, users may find themselves providing nominal consent to data practices with which they feel uncomfortable in order to access a digital platform's services.<sup>62</sup>

Users do often freely share their personal data. For example, users often post personal information on social network websites; in many other instances, they consent to the collection of their personal data by businesses and service providers. However, that consent is generally limited to the transaction at hand—for example, to enable lenders to evaluate mortgage apps or companies to ship items purchased online. Rarely, if ever, are users asked about the aggregation of their data for secondary uses—uses that they likely do not even contemplate when their data is first collected. Nevertheless, users are considered to have agreed to such uses because the consent in ToS and PPA is so broad that it includes almost every action that can be taken with users' information.<sup>63</sup> Such broad consent cannot constitute specific and informed consent as the app provider does not clarify specific information regarding data usage, but rather provides only general information. This leads to a situation in which users are not aware of the uses to which they are agreeing.

Various regulators are aware of this risk and have tried to limit it in legislation. For example, GDPR Article 6(4) stipulates the purpose limita-

---

61. *Id.*

62. See AUSTRALIAN COMPETITION & CONSUMER COMM'N, DIGITAL PLATFORMS INQUIRY FINAL REPORT, at 400 (2019).

63. See Kemp, *supra* note 39, at 643–44, 647–49.

tion principle, which is further elaborated in recital 50.<sup>64</sup> This principle specifies that personal data should only be collected for the specific purpose that is indicated to the user in advance, and that the data should not be used for any other purpose. “Vague and abstract purposes, such as ‘promoting consumer satisfaction,’ ‘product development’ or ‘optimizing services,’ are prohibited.”<sup>65</sup> Article 5 of the GDPR additionally references this risk principles relating to the processing of personal data. According to the Article, user information processing should be “for specified, explicit, and legitimate purposes[,]” and the information should not be further processed in a manner that is incompatible with those purposes. The CCPA also refers to this ethical risk in section 1798.100(b).<sup>66</sup> According to this section, the user must be informed of the purpose for which the information was collected; however, there is no reference to the fact that the purpose needs to be specific. In the CPRA, there is an extension of section 1798.100(b) in section 1798.100(b)(2), which stipulates that a company shall not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that do not match the disclosed purpose for which the sensitive personal information was collected, without providing the consumer with a notice consistent with section 1798.100(b)(2).<sup>67</sup>

Nevertheless, app providers often set very broad definitions for the purpose of collecting information, such as “the legitimate uses of the app” or “necessary to provide services.” Because this terminology might give the user the positive impression that app providers are only collecting information necessary to provide services and are only using the data for legitimate purposes, it is unethical. Such a definition enables data collection for a wide range of purposes without providing users a genuine explanation about what information is collected about them and for what purposes.

## ii. Lack of Transparency

A key data protection risk is lack of transparency. Many apps fail to meaningfully inform their potential users about the types of personal data that the app may process, as well as the purposes of data processing. Other app providers are silent on these matters. Therefore, ToS and PPA do not enable users to understand the extent of risk of using a certain app.<sup>68</sup> The lack of transparency is closely related to a lack of free and

64. See GDPR, *supra* note 15, recital 50.

65. See Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. COMM. TECH. L. 65, 77–78 (2019); Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1005–09 (2017).

66. CAL. CIV. CODE § 1798.100(b).

67. *Id.* § 1798.100(b)(2).

68. See, e.g., FUTURE OF PRIVACY FORUM, *June 2012 FPF Mobile Apps Study* (2012); Candida Leone, *Transparency Revisited—on the Role of Information in the Re-*

informed consent. When users receive only partial information about an app and the possible risks of using it, they cannot make an informed decision about whether to use the app.<sup>69</sup>

When it comes to transparency, individuals must be given clear information on what data is processed, including data observed or inferred about them. Further, users should be better informed on how, and for what purposes, their information is used. This transparency should include, when relevant, the logic used in algorithms that produce assumptions and predictions about them. Many app providers do not offer this information to the user.<sup>70</sup> Examples of this lack of transparency are evident in ToS and PPA of various widely used apps such as Twitter, WhatsApp, and Dropbox, all of which are silent on many ethical risks, inter alia, how user information is processed, how the app provider secures user information, and complete purposes of user information.

The GDPR stipulates that individuals have a right to be informed about the collection and use of their data. This provision has led to a variety of information obligations by the app provider. The law differentiates between two cases: personal data that is directly obtained from the data subject and personal data that is indirectly obtained.<sup>71</sup> When data is obtained directly from data subjects, individuals must be immediately informed about processing purposes and legal bases, any intentions to transfer personal data to third parties, the duration of storage, their own rights, the ability to withdraw consent, the right to complain about the authorities, and more. If personal data is not obtained directly from data subjects, users must be provided with the aforementioned information within a reasonable time period (i.e., within a month at most).<sup>72</sup>

The CCPA refers to this ethical risk of lack of transparency in section 1798.110, which defines a list of issues about which users have the right to receive information from the businesses that collect their personal data.<sup>73</sup> These topics include the type of personal information collected, categories of sources from which personal information is collected, the purpose

---

*cent Case-Law of the CJEU*, 10 EUR. REV. CONT. L. 312 (2014); Marco Loos & Joasia Luzak, *Wanted: A Bigger Stick. On Unfair Terms in Consumer Contracts with Online Service Providers*, 39 J. CONSUMER POL'Y. 63, 86–88 (2016); Ellen Wauters et al., *Optimizing Transparency for Users in Social Networking Sites*, INFO, Sept. 2014, at 8; Thomas Wilhelmsson, *Cooperation and Competition Regarding Standard Contract Terms in Consumer Contracts*, 17 EUR. BUS. L. REV. 49, 55 (2006).

69. See Omri Ben-Shahar & Adam Chilton, *Simplification of Privacy Disclosures: An Experimental Test*, 45 J. LEGAL STUD. S41, S42 (2016); Hoofnagle et al., *supra* note 65, at 77.

70. See European Data Prot. Supervisor, *Opinion 7/2015, Meeting the Challenges of Big Data*, at 6 (Nov. 19, 2015), [https://edps.europa.eu/sites/edp/files/publication/15-11-19\\_big\\_data\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf) [https://perma.cc/6NND-8B3Y].

71. These two circumstances are referenced in Article 13 and Article 14 of the GDPR, respectively. GDPR, *supra* note 15, Articles 13–14.

72. *Id.* Article 14.

73. CAL. CIV. CODE § 1798.110.



for which information is collected, third parties that can access to the information, and more.

b. Limited User Data Control

Within this risk, a number of secondary risks can be included, which increase the power gaps between users and app providers and limit the power of users to control their information and also to provide free and informed consent to use the application. The risks are:

i. Inability to Delete User Account Data

Under Article 17 of the GDPR, individuals have the right to have personal data erased. This right is also known as the “right to be forgotten.”<sup>74</sup> Users have a right to data erasure when their personal data has been unlawfully processed or is no longer necessary for processing purposes, or when the information is inaccurate or no longer relevant. The right to erasure also applies when data subjects withdraw consent.<sup>75</sup>

Like the GDPR, the CCPA also gives users the right to delete information about themselves and obligates businesses to notify users of their right to delete their information. This right is specified in section 1798.105.<sup>76</sup> The CPRA requires businesses to provide additional mechanisms for individuals to access, correct, or delete data, with a particular focus on information used by automated decision-making systems.<sup>77</sup>

Although required by law, some companies fail to comply with these obligations and do not allow their users to delete information that has been collected from their accounts. Some companies do erase the information, but they go about it unethically; they may take a long time to delete the personal data, or require users to go through a complex procedure to have their data erased.<sup>78</sup>

Examples of violations of the right for users to delete their account data and unethical behavior can be found in a study that looked at the data deletion mechanisms presented in the privacy policies of 108 websites. According to the study:

41 websites offered the option to have the account permanently deleted, and 13 allowed visitors to temporarily suspend or deactivate their account . . . . Ninety of 108 websites offering deletion

74. See Jerome Squires, Note, *Google Spain SL v Agencia Española de Protección de Datos* (European Court of Justice, C-131/12, 13 May 2014), 35 ADEL. L. REV. 463 (2014).

75. See Hoofnagle et al., *supra* note 65, at 78.

76. CAL. CIV. CODE § 1798.105 (West 2020).

77. Reference to these issues is found in sections 1798.105, 1798.130, and 1798.145.

78. See Hana Habib et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, in FIFTEENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 387, 395 (2019), <https://www.usenix.org/system/files/soups2019-habib.pdf> [<https://perma.cc/S5JN-QBBQ>].

did not describe a time frame in which a user's account would be permanently deleted and only four policies stated that information related to the account would be deleted "immediately." Another three claimed the time frame to be 30 days, and two websites said the deletion process could take up to one year.<sup>79</sup>

ii. Inability to Condition Over a Specific Clause

The choice to accept ToS and PPA is often binary; in other words, people are forced to either accept ToS and PPA as a whole or forego the possibility of using the web or mobile app altogether.<sup>80</sup> Users cannot provide their consent to only specific provisions of PPA and ToS. Therefore, by accepting the agreements, they agree to all the terms. For this reason, users often have no means of influencing the content of PPA and ToS.<sup>81</sup> The risk of inability to condition over a specific clause is not mentioned in the GDPR, the Consumer Rights Directive of the EU, the CCPA, or the CPRA.

iii. Content Removal Clause

A content removal clause specifies the conditions under which service providers may remove user content. User content refers to the content that users create, and it is considered to be their intellectual property. Users have the expectation that content they have created or uploaded to an app is their own, and that they will not be denied access (or ownership) to it. However, many apps operate unethically and state in their ToS and PPA that they can remove user content at their discretion without notifying users in advance or obtaining their consent.<sup>82</sup> As such, they limit users' power over the content they create in the app and, as a result, they limit users' proprietary rights and hurt users' reasonable expectation of having unrestricted access to content created by them.

App providers should define the specific conditions under which user content will be justly removed. It is unethical if providers may remove user content at their sole discretion, at any time and for any or no reason, without notifying users or providing the possibility for users to retrieve the content. App providers must respect users as content creators, as well as users' property rights over the content. The issue of involuntary user con-

79. *Id.* at 395.

80. See SANCHARI DAS ET AL., *Privacy Preserving Policy Framework: User-Aware and User-Driven*, at 2 (2019).

81. See Fred H. Cate, *The Limits of Notice and Choice*, 8 IEEE SECURITY & PRIV. 59, at 60 (2010); Marco Lippi et al., *CLAUDETTE: An Automated Detector of Potentially Unfair Clauses in Online Terms of Service*, 27 ARTIFICIAL INTELLIGENCE & L. 117, at 119, 125 (2019); Florian Schaub et al., *Designing Effective Privacy Notices and Controls*, 21 IEEE INTERNET COMPUTING 70, at 72 (2017).

82. See Marco Lippi et al., *Automated Detection of Unfair Clauses in Online Consumer Contracts*, in LEGAL KNOWLEDGE AND INFORMATION SYSTEMS 145, 145–54 (Adam Wyner & Giovanni Casini eds., 2017); Lippi et al., *supra* note 81.

tent removal is not addressed in the GDPR, the Consumer Rights Directive of the EU, the CCPA, or the CPRA.

iv. Unilateral Termination Clause

The unilateral termination clause gives app providers the right to suspend or terminate service or user contracts on their own initiative and for any reason without notifying the user. This clause only sometimes details the circumstances under which providers have this right.<sup>83</sup> Clauses stipulating that service providers may suspend or terminate the service at any time for any or no reason, and without notice to the users, are unethical because such behavior would create constant uncertainty for users. Users chose to use the app, added personal content to it, and established personal assets in it. Users are thus dependent on the service provided by the app and expect to continue receiving this service. However, this clause allows app providers the ability to suddenly decide to suspend or terminate the service. If users knew what behaviors would end service delivery, they could avoid those behaviors, and they would assume responsibility if the service was terminated due to unwanted behavior. However, if app providers can terminate service for any reason, users do not have the ability to exert any control or to know when to expect service termination.<sup>84</sup> The risk of the unilateral termination clause is not considered in the GDPR, the Consumer Rights Directive of the EU, the CCPA, or the CPRA.

v. Unilateral Change Clause

The unilateral change clause specifies the conditions under which service providers can amend and modify ToS or the service itself. ToS and PPA that users agree to at the beginning of service will not necessarily be valid when users decide to disconnect from the app or make changes to their accounts.<sup>85</sup> Such a clause has always been considered potentially unfair because it protects service providers against any claims by users regarding the service and terms.<sup>86</sup> App providers are given the opportunity to pass responsibility onto users to log in and review the updated terms periodically. Given the number of apps with PPA and ToS that users sign, it is impossible for any individual users to keep themselves informed of the new terms in this way.<sup>87</sup> A typical unilateral change clause includes

83. See Lippi et al., *supra* note 81, at 125.

84. See Simon Bradshaw et al., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, 19 INT'L. J.L. & INFO. TECH. 187, 203–04 (2011) (discussing data preservation issues after contract termination); Loos & Luzak, *supra* note 68, at 74–75.

85. See Loos & Luzak, *supra* note 68, at 67–72 (discussing unilateral changes of contractual terms by online service providers).

86. See Lippi et al., *supra* note 82, at 149.

87. See Yair Amichai-Hamburger & Oren Perez, *Anonymity and Interactivity on the Net: The Right to Privacy as a Multi-Dimensional Concept*, in PRIVACY IN AN ERA OF CHANGE 201 (Tehilla Schwartz Altshuler ed., 2012) (Hebrew); Kemp, *supra* note 39.

sentences like, “The services may change from time to time, at our discretion”; “We retain the right to create limits on use and storage at our sole discretion at any time; or “We may revise these terms from time to time.”<sup>88</sup>

This risk demonstrates the extreme power gap that exists between users and app providers. Additionally, the risk also directly concerns the matter of consent. After all, when app providers make a change to the agreement without notifying users of the change, it effectively means that the change occurs without user consent, and therefore, reflects a new contract. Even if app providers announce that they are modifying the agreement and allow users to decide if they choose to accept the new terms, it still may not be ethical. For example, if the new terms are worse for users than those included in the original agreement, and users have already developed a dependency on the app, most users will end up agreeing to the terms. Thus, this consent is considered uninformed consent.

The issue of the unilateral change clause is not addressed in the Consumer Rights Directive of the EU, the CCPA, or the CPRA. Although the GDPR does not address this risk directly, it may be that this practice undermines the conditions of informed consent and purpose limitation, two issues described earlier. In that case, the unilateral change clause may be prohibited under the GDPR, at least with respect to data practices. However, without a direct reference to the topic, users will not necessarily pay attention to the issue or realize that the issue is addressed in legislation.

#### vi. Unilateral Changes of Financial Charges

Many apps either indicate in their descriptive headline that they are free of charge or present the cost of usage in capital letters. However, ToS clauses may award the app provider a unilateral right to modify price terms. For example, a clause may state that there will be a financial charge for using the app a year after it is downloaded, or that certain services that the app provides will be charged for a fee. Such clauses are considered unethical if ToS does not specify the conditions under which the price may be changed and the criteria for calculating the change.<sup>89</sup> Also, such clauses are considered unethical if users do not have the right to terminate the contract after having been informed that the app provider indeed wishes to charge a fee.<sup>90</sup> The risk of the unilateral changes of financial charges is not addressed in the GDPR, the Consumer Rights Directive of the EU, the CCPA, or the CPRA.

---

88. See Lippi et al., *supra* note 82, at 148–49.

89. See Oliver Gerstenberg, *Constitutional Reasoning in Private Law: The Role of the CJEU in Adjudicating Unfair Terms in Consumer Contracts*, 21 EUR. L.J. 599 (2015); Bert Keirsbilck, *The Erga Omnes Effect of the Finding of an Unfair Contract Term: Nemzeti*, 50 COMMON MKT. L. REV. 1467, 1471–72 (2013).

90. See Loos & Luzak, *supra* note 68, at 68–69; Peter Rott, *The Adjustment of Long-Term Supply Contracts: Experience from German Gas Price Case Law*, 21 EUR. REV. PRIVATE L. 717 (2013).

## 2. *Restricting User Legal Action*

According to Article 3 of the Council Directive 93/13/EEC from April 5, 1993, on unfair terms in consumer contracts, a contractual term is unethical if “contrary to the requirement of good faith, it causes a significant imbalance in the parties’ rights and obligations arising under the contract, to the detriment of the consumer.”<sup>91</sup> Companies include provisions in their PPA and ToS that may be unethical if their content is unexpected from the point of view of the users, or if they limit legal action in a prohibitive way that undermines consumer protection or privacy protection. These provisions include mandatory arbitration, choice of law, choice of jurisdiction, and limitation of liability, as detailed below.

This primary risk and its secondary risks are not addressed under the four laws. The GDPR, the CCPA, and CPRA do not refer to these risks at all. The Consumer Rights Directive of the EU also does not address this primary risk and its secondary risks, but it does direct each state to consider these risks in accordance with state laws of both consumer protection and contract law. These risks are addressed in other laws, such as laws that deal with contracts in general, and uniform contracts in particular. However, from the users’ points of view, this is problematic because reasonable users without legal knowledge will seek to determine their legal rights in legislation that is most relevant to the document that they are reading. For example, the Consumer Protection Law is most relevant to ToS and the Privacy Protection Law is most relevant to PPA. In practice, however, the reference to risks is scattered across various pieces of legislation, so it becomes very difficult for users to determine their rights according to legislation. This issue raises another unethical behavior: there is no single piece of legislation that users can review to understand their rights under PPA and ToS.

### a. Mandatory Arbitration

Mandatory binding arbitration is a contract provision that requires the parties to resolve disputes regarding the contract through arbitration rather than through the court system or other forms of dispute resolution.<sup>92</sup> Mandatory binding arbitration may require the parties to waive specific rights, such as their right to appeal a decision.<sup>93</sup> Moreover, ToS determine the specific arbitration forum and the procedural and evidentiary rules that will apply. Because these provisions might not be easily discoverable in agreements, and many people do not know or reasonably expect that a contract would remove their ability to pursue an issue in

---

91. Directive 2011/83/EU, *supra* note 24.

92. See Lippi et al., *supra* note 82, at 149–50; Lippi et al., *supra* note 81, at 126–27; Mitchell Grant, *Mandatory Binding Arbitration Definition*, INVESTOPEDIA, <https://www.investopedia.com/terms/m/mandatory-binding-arbitration.asp> [https://perma.cc/SM3F-NREN] (last updated Apr. 20, 2021).

93. *Supra* note 92.

court, many people are not aware that their rights may be significantly curtailed with the acceptance of the agreements.<sup>94</sup>

The U.S. court system has approved the use of binding arbitration clauses in consumer contracts. For example, according to case law parties may agree to arbitration under the Federal Rules of Civil Procedure, or under a competing disclosure proceeding in legal proceedings.<sup>95</sup> The Supreme Court has held that arbitration is a matter of contract, and the Federal Arbitration Act (FAA) requires the courts to respect the contract to which both parties agreed. Although such a clause may be legal, it still may be unethical in certain cases. For example, clauses may state that arbitration takes place in a state other than the state of the user's residence and or that arbitration is based on an alternative set of rules.<sup>96</sup>

#### b. Choice of Law

A choice of law clause specifies the law governing the relations arising from the agreement, and the law by which a potential dispute will be adjudicated.<sup>97</sup> Many apps state that the governing law is of the country in which their parent company operates. A question arises as to whether such a provision can reasonably be expected by the user, and whether it is enforceable. In Israel, the supreme court has ruled in a case involving Facebook that, as a rule, the choice of law clause is valid.<sup>98</sup> However, if the choice of law clause deprives the user of the possibility to make certain claims, and in cases in which the law is not accessible to the user or does not have similar characteristics to Israeli law, the choice of law clause may be regarded as a depriving condition in a standard contract and, as such, may be canceled. According to this judgment, a choice of law clause may be unethical in cases where the law is not accessible to the user (e.g., when the clause follows the law of an unfamiliar state that a reasonable user would not expect, or the law of a state is reputed to have very weak consumer protection laws). Additionally, the clause may be unethical in cases in which it prevents the user from raising claims that form the root of the legal process, such as states that do not allow filing class actions, or in which the clause according to which the user wants to sue does not exist.<sup>99</sup>

#### c. Choice of Jurisdiction

A jurisdiction clause specifies the courts that will adjudicate the disputes arising from the contract. A clause is unethical when it determines that jurisdiction is limited to a specific place, such as in the city or state

94. See David S. Schwartz, *Mandatory Arbitration and Fairness*, 84 NOTRE DAME L. REV. 1247 (2009); Jean R. Sternlight, *Creeping Mandatory Arbitration: Is It Just?*, 57 STAN. L. REV. 1631 (2005).

95. See AT&T Mobility LLC v. Concepcion, 563 U.S. 333 (2011).

96. *Id.* at 342–43, 358–59, 364, 366.

97. See Lippi et al., *supra* note 82, at 148; Lippi et al., *supra* note 81, at 122–23.

98. REA 5860/16 Facebook Inc. v. Ohad Ben Hamu, (2018) (Isr.).

99. See Loos & Luzak, *supra* note 68, at 84–86.

where the parent company of the app is located, regardless of the place of residence of the user.<sup>100</sup> In Israel, the court ruled in the Facebook case that the forum clause is not valid because users cannot reasonably be expected to file their lawsuit in California.

#### d. Limitation of Liability

A limitation of liability clause specifies the amount and types of damages that an app provider will be obligated to provide to users under the terms and conditions stated in the service agreement. Additionally, it states that the duty to pay damages is limited or excluded for certain kinds of losses, under certain conditions. In ToS and PPA, many clauses reduce and limit the liability of the service provider for damages (such as any harm caused to the computer system because of malware or loss of data) and for the suspension, modification, discontinuance, or lack of availability of service.<sup>101</sup> The boundary between an ethical clause and an unethical clause is based on the number of issues that app providers remove from their liability; as the number of excluded liability issues increases, the clause becomes more unethical.<sup>102</sup>

### 3. *Limited Readability*

According to Article 5 of the Council Directive 93/13/EEC from April 5, 1993, on unfair terms in consumer contracts, “terms must always be drafted in plain, intelligible language.”<sup>103</sup> However, one of the main reasons that users do not read PPA and ToS is their complex language, which includes legal jargon that obscures the basic meaning of terms and misleads users. Additionally, these documents are long and difficult to navigate, as detailed below in the description of secondary risks.<sup>104</sup> The agreements are structurally complex for users and difficult to understand, obstructing informed consent even if users do choose to read them. This lack of understanding makes users’ consent a risk in and of itself and highlights their lack of control in comparison to app providers.

The difficulty in understanding and reading ToS and PPA is exacerbated by the fact that these agreements are signed on a small mobile phone screen. Various studies have indicated that people’s attention when making decisions in front of a mobile phone screen is much lower than when they make decisions in front of a computer screen. This reduc-

---

100. See Lippi et al., *supra* note 82, at 148; Lippi et al., *supra* note 81, at 122.

101. See Lippi et al., *supra* note 82, at 149; Lippi et al., *supra* note 81, at 123–24.

102. See Loos & Luzak, *supra* note 68, at 79–81.

103. See Article 5 of the Council Directive 93/13/EEC from April 5, 1993.

104. See Bakos et al., *supra* note 33, at 31–32; Lior Jacob Strahilevitz & Matthew B. Kugler, *Is Privacy Policy Language Irrelevant to Consumers?*, 45 J. LEGAL STUD. 569 (2016).

tion in attention thus affects the ability to carefully read the documents, as well as the ability to understand them.<sup>105</sup>

The risk of limited readability and its secondary risks are addressed in neither the Consumer Rights Directive of the EU nor the CCPA. In the GDPR, this risk and its secondary risks are not discussed directly, but the principles of purpose limitation and informed consent, which have been extensively mentioned previously, require clear and comprehensible language. However, even though the GDPR addresses this issue indirectly, users would reasonably expect to see a direct reference to the topic. Without a direct reference, users may not know that the issue is addressed in legislation. The CPRA addresses this risk in several specific sections. For example, one section of the CPRA states that a company must provide a clear and conspicuous link on the business's Internet homepage(s), titled "Do No Sell or Share My Personal Information" or "Limit the Use of My Sensitive Personal Information."<sup>106</sup> Another section states that the company must provide specific pieces of personal information obtained from the consumer in a format that is easily understandable to the average consumer, and, to the extent that is technically feasible, in a structured, commonly used, machine-readable format, which also may be transmitted to another entity at the consumer's request without hindrance.<sup>107</sup>

a. Ambiguity

PPA of digital platforms are often vague. A key example of vague language is the frequent use of the word "may" in digital platforms' privacy policies. The word "may" denote various meanings, including the expression of uncertainty, permission, possibility, intention, or hope.<sup>108</sup> When used in contract terms, including in a digital platform's ToS and PPA, the use of the word "may" give digital platforms significant discretion to perform, or not perform, the actions that follow that word. Users reading a policy with this language, therefore, cannot accurately determine the exact scope of the user data that the platform will collect from them or how the data will be used and disclosed.<sup>109</sup>

---

105. See Shlomo Benartzi & Jonah Lehrer, *THE SMARTER SCREEN: SURPRISING WAYS TO INFLUENCE AND IMPROVE ONLINE BEHAVIOR* 40–43 (2015); Ayelet Sela, *E-Nudging Justice: The Role of Digital Choice Architecture in Online Courts*, 2019 J. DISP. RESOL. 127, 144–45 (2019).

106. Cal. Civ. Code § 1798.135 (West 2020).

107. *Id.* §1798.130.

108. See DIGITAL PLATFORMS INQUIRY FINAL REPORT, *supra* note 62, at 405–06.

109. See Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S J.L. & POL'Y INFO. SOC'Y 425 (2010); Reidenberg et al., *supra* note 12; Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370 (2013).



## b. Complexity

PPA and ToS of digital platforms are often complex. The complexity of language makes it difficult for average users to process the information contained within these policies<sup>110</sup> and to decide on a useful course of action if there is a problem.

## c. Length

PPA and ToS of digital platforms often span many pages; as such, if a user chose to read them, it would take a long time.<sup>111</sup> A review by the Australian Competition Consumer Commission (ACCC) found that “each digital platform’s privacy policies, excluding the additional links to separate web pages, were between 2,500 and 4,500 words, and would take an average reader between 10 and 20 minutes to read. These average reading times are likely to significantly exceed the time actually spent by consumers trying to read digital platforms’ privacy policies.”<sup>112</sup>

## d. Misleading or Unclear Language

The risk of misleading or unclear language refers to the use of sophisticated words and complicated sentences in ToS and PPA. This language obscures the underlying meaning of the terms used and misleads users.<sup>113</sup> Many apps use terms such as “granting the right to erase information,” “allowing information to be corrected,” “using the information only for the purposes for which it was collected,” and more. In practice, however, users are not provided with the tools needed to exercise such rights. Thus, a situation is created in which users believe they are granted many rights in an agreement, yet, in practice, it would be impossible for them to carry out any legal action.

For example, one study that looked at 150 websites found that, in six instances, the text in a privacy policy referred to an opt-out option, but that option either did not exist or the website did not provide vital information to opt out, such as an email address for sending privacy requests. Additionally, six websites included misleading information in the privacy policy text. Finally, seven websites mentioned user accounts in PPA, but no mechanisms to create a user account were found on the website.<sup>114</sup>

---

110. See DIGITAL PLATFORMS INQUIRY FINAL REPORT, *supra* note 62, at 405; Ben-Shahar & Chilton, *supra* note 69; Yaniv Roznai & Nativ Mordechay, *Access to Justice 2.0: Access to Legislation and Beyond*, 3 THEORY & PRAC. LEGIS. 333 (2015).

111. See Aleecia M. McDonald & Lorrie Faith Cranor, Article, *The Cost of Reading Privacy Policies*, 4 I/S A J. L. & POL’Y INFO. SOC’Y 543 (2008).

112. DIGITAL PLATFORMS INQUIRY FINAL REPORT, *supra* note 62, at 403 (footnote omitted).

113. See Bakos et al., *supra* note 33.

114. See Habib et al., *supra* note 78, at 396.

## e. Difficulty of Navigation

Many digital platforms' terms and conditions are hard to navigate because of numerous and separate interlinked policies that all contain information regarding the digital platform's data practices. To understand all the content that ToS and PPA include, users must additionally read ToS and PPA of other apps to which ToS and PPA of the app-in-question refer. Given that each ToS and PPA is long in itself, the additional references make reading the entire content of ToS and PPA impossible for users.<sup>115</sup> This is an ethical risk as this type of practice requires users to also be associated with the agreements of other apps because they have given consent to use a specific app that is bound by additional agreements. As such, users are compelled to commit to a contract outside of the one to which they have directly consented. Further, terms and conditions are often presented in a way that is hard to navigate due to disorganized typographic aspects (e.g., small font size, compressed line height, shortened line length).<sup>116</sup>

## 4. Profiling

Profiling refers to the process of constructing a user profile based on computerized data analysis. More specifically, this process refers to the use of algorithms or other mathematical methods to uncover patterns or correlations within large quantities of data, which are then aggregated in databases. When these patterns or correlations are used to identify or represent people, they are called profiles. Profiles can then be used to draw inferences and personalize content and services. Due to people's limited understanding of data protection and user information tracking, an enormous amount of information about them can become available to multiple bodies, ranging from advertisers, service providers and other commercial entities, to governments. This, in turn, allows those bodies to build profiles of individuals with the aim of targeted advertising, targeted treatments, or other means of persuasion.<sup>117</sup>

The GDPR addresses the risk of profiling, and its secondary risks, in two main sections: (1) Article 4 (a section that legally defines profiling) and (2) Recital 71 (a section that outlines what should not be done with user profiles). In these sections, the law tries to protect users from the creation of profiles by only allowing automated processing of information that could be used to tag a user as a part of a specific group. In the case of profiling, the law tries to address both primary and secondary risks, and even to prevent discriminatory effects on persons based on a number of criteria, including racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic aspects, and health status. The

115. See DIGITAL PLATFORMS INQUIRY FINAL REPORT, *supra* note 62, at 406.

116. See *id.*

117. See Sumitkumar Kanoje et al., *User Profiling Trends, Techniques and Applications*, 1 INT'L J. ADVANCE FOUND. RES. COMPUTER 119 (2014).

CCPA is silent in regard to these primary and secondary risks. The CPRA addresses the risk of profiling in section 1798.140, the definitions section, which describes the profile of any type of automated processing of personal information for the assessment of certain personal aspects relating to a natural person, and in particular for the analysis or prediction of related aspects. According to this law, profiling includes “natural person’s performance at work, economic status, health, personal preferences, interests, reliability, behavior, location, or movements.”<sup>118</sup> Also, in the regulatory section, section 1798.185 (16) states that regulations on access and rights of revocation of consent should be installed in relation to the business use of automated decision-making technology, including profile.<sup>119</sup>

The risk of the creation of user profiles is twofold. First, problematic use can be made of profiles; and second, the very existence of user profiles is a risk. These risks are described in the following secondary risks.

a. Creation of User Profiles that Negatively Affect Future Opportunities

Through profiles, people are tagged in particular groups, which then expose them to receiving particular online publications and internet search suggestions. Once a user profile is customized, all advertisements, sentence completions in web searches, and offered services will be targeted to the user profile. Through this process, the “choices” presented to any particular user end up being based on assumptions about them. Those “choices” then determine to which circle the user will belong, thus creating a recurrent loop reaffirming the user’s belonging to that same group, making it difficult to gain exposure to additional choices and opportunities.<sup>120</sup>

An individual’s development depends on the opportunities that the individual is either given or denied. In the context of big data, several academics have expressed concerns over the kind of personalization that occurs with user profiles, particularly how it can narrow people’s life opportunities in discriminatory ways. Predictive algorithms rely on mined data in order to “learn” from the user’s past; these algorithms operate by analyzing data and uncovering statistically significant patterns.<sup>121</sup> The individual user’s past is based on assumptions that the respective algorithms have discovered—for example a person’s physical characteristics, preferences, habits, personality traits, and any other type of information that is being tracked and can be inferred.<sup>122</sup> Based on this past, the algorithm

---

118. Cal. Civ. Code § 1798.140 (West 2020).

119. *Id.* § 1798.185 (16).

120. See Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904 (2012); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2012).

121. See Solon Barocas & Andrew D. Selbst, *Big Data’s Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

122. See Michal Kosinski et al., *Private Traits and Attributes Are Predictable from Digital Records of Human Behavior*, 110 PROC. NAT’L ACAD. SCI. 5802 (2013).

conducts predictive analyses and determines the choices that individuals will be given.<sup>123</sup> In turn, these same “choices” that were presented and based on prior assumptions are also the choices that determine the subsequent assumptions, creating a circular framework. As such, users remain within the group in which they were tagged and do not aspire to advance.<sup>124</sup> Sometimes big data is used to make determinations about individuals; however, these determinations are not based on concrete facts, and rather on inferences or correlations that may be unwarranted. Individuals may be judged not based on what they have done or what they will do in the future, but on inferences or correlations drawn by algorithms. These inferences subsequently may suggest to others that the individual has poor credit or that they will be an insurance risk, that they may be unsuitable candidates for employment or university admission, and more.<sup>125</sup>

b. Personal Information that May Be Used to Discriminate

The aggregation and disclosure of users’ personal information that occurs in the process of user profiling and segmenting can lead to discrimination, based on users’ online and offline behavior.<sup>126</sup> This information can be used to draw unexpected and negative conclusions about users that can cause them harm within society and exacerbate social inequality and distributive injustice. Profiling allows marketers and retailers to segment users into distinct groups based on their relative value and expected profitability to retailers. Thus, weak populations are pushed aside and end up receiving fewer quality products across all types of services, including in the medical field. This leads to a situation in which the wealthy receive better medical care, including state-of-the-art technologies and more senior and qualified doctors. Discrimination also occurs in credit ratings (data on users’ purchases on the Internet is collected to create a credit rating profile), which leads to particular users being charged more for services based on their perceived ability to pay. For example, users who are perceived unable to pay may be charged higher interest rates or insurance premiums. Segmentation in the online world, therefore, produces and reinforces societal inequalities.<sup>127</sup>

123. See Tene & Polonetsky, *supra* note 120, at 239, 253.

124. See Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 *FORDHAM INTELL. PROP. MEDIA ENT. L.J.* 803 (2016).

125. See Marijn Sax, *Privacy from an Ethical Perspective*, in *THE HANDBOOK OF PRIVACY STUDIES: AN INTERDISCIPLINARY INTRODUCTION* 143–72 (Bart van der Sloot & Aviva de Groot eds., 2018).

126. See Kemp, *supra* note 39, at 648–52.

127. See Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 *J. TECH. L. & POL’Y* 41 (2014); Christopher Townley, Eric Morrison & Karen Yeung, *Big Data and Personalized Price Discrimination in EU Competition Law*, 36 *Y.B. EUR. L.* 683 (2017); Karen Yeung, *Five Fears About Mass Predictive Personalization in an Age of Surveillance Capitalism*, 8 *INT’L DATA PRIVACY L.* 258 (2018).

c. Using Profiles for Undeclared Purposes

One may assume that ethical and trustworthy service providers would use information collected from user profiles only if they had users' explicit consent, and that they would use that information solely for purposes specified and only for the benefit of the users. However, there are service providers who are less inclined to protect user data and who may use user profiles for undeclared purposes. This behavior is unethical as users will not anticipate the use of their profiles for other needs and will have no way of controlling how their profile will be used.<sup>128</sup>

d. Creation of Aggregated Profiles

First-party data profiles refer to any user information that is collected and synthesized by advertisers themselves. However, many times advertisers lack data on prospective customers and turn to third-party data profiles. Third-party data profiles are based on aggregated information from varied data pieces and sources that are unknown to the advertiser. Data profiles collected by third parties are based on a subset of the population and are formed according to the way the advertiser brands users and not according to the true characterization of groups. As a consequence, advertisers receive processed profiles, which they then use to create user profiles. As such, the connection between the initially collected information and the final profile that is created is accidental.<sup>129</sup>

5. *Processing User Information*

In general, data processing refers to the collection and manipulation of data items to produce meaningful information and may involve various actions, including collection, recording, validation, sorting, summarization, aggregation, classification, and more. According to the GDPR "processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."<sup>130</sup>

The personal data processing risk has earned senior status and broad protection in the GDPR, which regards the processing of user information

128. See Omar Hasan et al., *A Discussion of Privacy Challenges in User Profiling with Big Data Techniques: The EEXCESS Use Case*, in 2013 IEEE INTERNATIONAL CONGRESS ON BIG DATA 25 (2013); Jamie Yap, *User Profiling Fears Real but Paranoia Unnecessary*, ZDNET (Sept. 12, 2011), <https://www.zdnet.com/article/user-profiling-fears-real-but-paranoia-unnecessary/> [<https://perma.cc/8SF6-APAW>].

129. See Nico Neumann et al., *Frontiers: How Effective Is Third-Party Consumer Profiling? Evidence from Field Studies*, 38 *MARKETING SCI.* 918 (2019); Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 *J. LEGAL STUD.* S163 (2016).

130. See GDPR, *supra* note 15, Article 4(2).

as being subject to one of the core protections of privacy; therefore, the GDPR addresses the matter of processing across various sections.<sup>131</sup> According to Article 6 of the GDPR, the first principle of data protection requires that all personal data be processed lawfully, fairly, and transparently. A legal (or lawful) basis for processing must be obtained before an organization can process any personal data. The GDPR outlines six scenarios in which data processing is legally permitted. Unless an organization can show that the personal data processing activity fits within one or more of these scenarios, the action is deemed unlawful. The six legal bases for data processing are:

- (1) Data subjects have given consent to the processing of their personal data for one or more specific purposes.
- (2) Processing is necessary to carry out a contract to which the data subjects are a party.
- (3) Processing is necessary for compliance with a legal obligation to which the app provider is subject.
- (4) Processing is necessary to protect the vital interests of the data subjects.
- (5) Processing is necessary for the performance of a task carried out in the public interest.
- (6) Processing is necessary for legitimate interests pursued by the app provider or by a third party, except when such interests override the interests or fundamental rights and freedoms, or when the data subject is a child.<sup>132</sup>

In the CCPA, unlike the GDPR, there is no specific reference to information processing. The definition of processing in the CCPA can be found in section 1798.140. According to the definition provided, the processing is “any operation or set of operations that are performed on . . . personal data” in a manner that renders the personal information no longer attributable to a specific user without the use of additional information.<sup>133</sup> The law refers to processing indirectly within other sections, including sections that define the purposes for the use of information or the provision of information to third parties. The CCPA, in section 1798.185 (dealing with regulation), obligates businesses that process consumers’ personal information to “[p]erform a cybersecurity audit on an annual basis.” The audit will define the scope of personal information processing and instances in which the processing may pose a significant risk to personal information. Such businesses must also file a risk assessment with the California Privacy Protection Agency on a regular basis with respect to the processing of their personal information, including whether the

---

131. *See id. passim.*

132. *See id.* Article 6; Hoofnagle et al., *supra* note 65.

133. CAL. CIV. CODE § 1798.140 (West 2020).

processing involves sensitive personal information and whether the benefits of processing the information outweigh its disadvantages.<sup>134</sup>

Many digital apps work in accordance with the law, but nonetheless process the information in an unethical manner. The following list of secondary risks details the ways that digital apps process information in an unethical manner:

a. Transforming Meta-Data Into Significant User Information

Big data does not start as big data; rather, it is assembled, bit by bit, from small pieces of data and becomes “big” only when compiled. When users decide to sign up for an app, they reveal basic information about themselves including name, phone number, and address. They also allow the app to access details on their device, including contact lists, current location, the photo gallery and more. Each of these items may individually appear innocent and technical, but the processing of this basic information reveals much about the user. For example, access to users’ current location, in combination with their home address, can indicate information regarding their life habits. Further, accessing users’ photo galleries in conjunction with their contact lists can reveal insights about the group of people with whom they socialize. App providers additionally use essential information to advertise relevant products to specific users, and sometimes even sell the information to other advertisers. The data generated from the technical information is very valuable. Many times, users are unaware that the basic information they have provided has been aggregated in such a way that becomes much more meaningful and then is used beyond the purposes for which it was provided. Such practices, on the part of app providers, are illegal and unethical.<sup>135</sup>

Another concern that is related to this risk is the issue of de-identification of personal information. Information that does not identify the subject of the information is not subject to the same limitations of the law and, as such, there is no restriction on its collection, processing, and use. App providers can collect technical information about users and, as long as they keep the information unspecific and anonymous, this type of data collection is permitted by law. However, due to numerous technological developments, big data has become even bigger, and data analytics have become more sophisticated, increasing the ability to de-anonymize data and make inferences from an accumulation of non-personal data. For this reason, concerns have been raised that third parties may try to cross-iden-

---

134. *Id.* § 1798.185.

135. See Edith Ramirez, Chairwoman, FTC, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View from The Lifeguard’s Chair (Aug. 19, 2013) (transcript available at [https://www.ftc.gov/sites/default/files/documents/public\\_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf](https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf) [<https://perma.cc/65EJ-WEDF>]); ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES AND THEIR CONSEQUENCES 176–78 (2014).

tify information from several sources so that they can, at least, partially override the mechanisms of anonymity and connect information from the database to a specific individual. Thus, the alleged unidentified technical information becomes identifiable and exposes personal and sensitive information about the user.<sup>136</sup>

The GDPR refers to this risk in recital 26 (“Not Applicable to Anonymous Data”) by noting that information that could identify the user is still protected, and specifically anonymized information that could become de-anonymized is protected as well. However, non-specific anonymous information is not protected.<sup>137</sup> The CCPA and the CPRA are silent regarding this secondary risk.

#### b. Aggregating and Combining User Information From Multiple Sources

As explained above, the lure of big data often carries with it the risk of unidentified technical or personal information becoming identifiable. Modern data practices allow app providers to aggregate personal data from multiple sources. Data aggregators compile immense quantities of personal information about individual users, using data acquired from app providers that have had direct contact with the users, as well as data acquired from other data brokers with whom the users have never communicated. This information can be used to make inferences about users’ personal characteristics to profile and categorize users, particularly in ways that can be used to compile lists of users to sell to other app providers and data brokers.<sup>138</sup>

This unanticipated collection and combination of information can reveal intimate details about the user’s sexual activity, sexual orientation, religion, political views, level of debt, alcohol or drug consumption, diseases, disorders, insecurities, behavioral biases, financial vulnerability—all details that the users would likely have never chosen to disclose to the provider of the downloaded app or other app providers that use the services of a data broker.<sup>139</sup> Aggregating user information from multiple sources without the user’s knowledge and consent is unethical. One example of aggregation is social network aggregation, a process in which companies collect data about users from various social networks such as Facebook, Instagram, and Twitter for various analyses and other tasks.<sup>140</sup> This practice is particularly problematic given the personal nature of these data. The GDPR is silent regarding this secondary risk. The CCPA and

136. For more information on the issue of de-identification, see Tal Z. Zarsky & Bar-Ziv Sharon, *Privacy’s Identity Crisis: Regulatory Strategies in The Age of De-Identification*, 2 L. SOC’Y & CULTURE 125 (2019) (Isr.) (Hebrew).

137. See GDPR, *supra* note 15, recital 26.

138. See René Arnold et al., *Informed Consent in Theorie und Praxis*, 39 DATENSCHUTZ UND DATENSICHERHEIT—DUD 730 (2015) (Ger); Kemp, *supra* note 39, at 648–52.

139. See Kemp, *supra* note 39, at 648.

140. See, e.g., U.S. Patent No. 7,188,153 (filed Aug. 25, 2006).



the CPRA define the term “aggregating user information” in section 1798.140 but do not refer to it beyond that.

#### 6. *Tracking User Information*

Nowadays people’s activities are continuously tracked. Cellphones have become surveillance tools and the various apps installed on them collect minute-to-minute information about location, activities, interactions, preferences, and daily routines.<sup>141</sup> Apps collect information about users for the purpose of monitoring their online behavior. Users may be aware that they are disclosing their name, address, mobile phone number, product preferences, and credit card details. However, they are much less likely to be aware that apps track their subsequent internet browsing history, the way they navigate other apps, and their locations. The information may include the links that users click on and how long they spend on any particular page, information about browsers and devices through which users access the app and browsing activity across different sites. Such detailed tracking grants app providers access to information about an individual user’s interests, shopping habits, problems they are facing, and more.<sup>142</sup> In other words, individuals are under constant surveillance.

Users are also typically oblivious to the fact that the data they provide is combined with other personal information collected from other apps and data aggregators. The original information disclosed by a user may seem innocuous, but when combined with continued and unanticipated tracking of additional behavior, that information can become jeopardizing.<sup>143</sup> When users are knowledgeable of the constant monitoring that occurs through their cellphones, regardless of the extent to which they are aware of it, they behave differently than if they are not being monitored; thus, we can deduce that the tracking of users violates their autonomy.<sup>144</sup>

The risk of tracking user information, and its secondary risk, are not addressed in the GDPR, the Consumer Rights Directive of the EU, the CCPA, or the CPRA.

##### a. Tracking User Activities While Users Are Not Using the App (Cookies)

The most well-known online tracking technology is online cookies. Cookies are small pieces of data that app providers store on users’ devices.

141. See Jose Pagliery, “*Super Cookies*” Track You, Even in Privacy Mode, CNN BUSINESS (Jan. 9, 2015), <https://money.cnn.com/2015/01/09/technology/security/super-cookies/index.html> [<https://perma.cc/6LTU-BTRW>].

142. See Michael D. Birnhack, *Privacy: A Snapshot*, 2 L. SOC’Y & CULTURE 9 (2019) (Isr.) (Hebrew); Mike Schroepfer, *An Update on Our Plans to Restrict Data Access on Facebook*, FACEBOOK (Apr. 4, 2018), <https://about.fb.com/news/2018/04/restricting-data-access/> [<https://perma.cc/WVU3-G52B>].

143. See Kemp, *supra* note 39.

144. See Cohen, *supra* note 120; Daniel J. Solove, “*I’ve Got Nothing to Hide*” and Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745 (2007).

Apps often use cookies to remember user preferences and deliver a personalized experience, as well as to gain information for advertising. Once an app has dropped a cookie on a user's computer, the app provider can continue to access that device; this is how apps can use cookies to track users from page to page or from site to site.<sup>145</sup>

First-party cookies are often used by webpages to recall information about users (for example, contents of their online shopping cart) and to personalize their experience (for example, displaying the time and weather at a user's location). A more problematic practice is the use of cookies by third parties (i.e., companies other than the one operating the app), often for advertising purposes and for tracking users across different sites.<sup>146</sup>

### 7. *Third-Party Data Transfers*

Third-party data sharing occurs when user data is transferred from one entity to another, or when one entity allows another entity to access its collection of user data. User data can be shared between digital platforms and a wide variety of third parties, including advertisers, researchers and academics, advertising partners, data analytics providers, and payment service providers. Large amounts of user data can also be shared between digital platforms and app developers.<sup>147</sup>

The main problem with transmitting information to third parties is that users lack control over their information. Users agree to the collection of information by a specific app, but this data may end up being transferred to many third parties of which users are not aware or with which they do not have an agreement about data retention. Thus, users have no way of knowing where the information ends up, nor whether it is properly secured and how it will be used.<sup>148</sup>

The GDPR defines the term "third party" in Article 4(10). Beyond providing a definition, the reference in the law to the issue of third parties is primarily focused on the transfer of data between countries and not between third parties in general or between subsidiaries. This is a general reference to the issue and not a specific reference that addresses the risk; therefore, reasonable users cannot determine their rights regarding this risk in this law.

The CCPA defines the term "third party" in section 1798.140(w). In addition, the CCPA addresses the sale or transfer of information to third

145. See DIGITAL PLATFORMS INQUIRY FINAL REPORT, *supra* note 62, at 387.

146. See *id.*; see also Bhatia, *supra* note 34; Loos Marco et al., *Regulation of Digital Content Contracts in the Optional Instrument of Contract Law*, 19 EUR. REV. PRIV. L. 729 (2011).

147. See Mark Scott & James Kanter, *European Officials Accuse Facebook of Misleading Them on WhatsApp Deal*, N.Y. TIMES (Dec. 20, 2016), <https://www.nytimes.com/2016/12/20/business/eu-facebook-whatsapp-vestager.html> [<https://perma.cc/2ZTU-RU3R>].

148. See DIGITAL PLATFORMS INQUIRY FINAL REPORT, *supra* note 62.

parties in section 1798.115, which deals with users' right to receive upon request disclosure of the sale of their personal information to third parties as well as the reasons for which the information was transferred. The section further specifies the ways that the information can be transmitted. Another section that relates to the sale or transfer of information to third parties is section 1798.120, which deals with a user's right to withdraw consent to the sale of their personal information to third parties. The CPRA adds in section 1798.140, the definitions section, a description of what is considered the sharing of personal information and states that any transfer of personal information to a party that is not a party to the contract (with or without payment) is considered sharing of the information.

#### IV. DISCUSSION AND APPLICATIONS

The Article has presented a typology of ethical risks arising from the content of ToS and PPA, identified through a qualitative review of relevant sources. The typology divides these ethical risks into seven categories of primary risks (each of which includes sub-risks): uninformed consent, restriction of user legal action, limited readability, profiling, processing user information, tracking user information, and third-party data transfers. These risks lead to a violation of individual autonomy,<sup>149</sup> and the undermining of users' self-determination, which are further accentuated by the fact that users are under constant surveillance.<sup>150</sup> Through tracking, app providers are able to gather a great deal of information about users, which is then processed into specific profiles per each user.<sup>151</sup> As such, the "choices" presented to users online are not actually user choices, but rather results based on assumptions about them and are a product of their profiling.<sup>152</sup> Further, the use of persuasive computing techniques creates a type of brainwashing, which consequently affects users' conduct and the choices they make in their lives.

True autonomy occurs when users have the ability to make independent and informed decisions. The manipulative introduction of information into the user environment fundamentally interferes with individual autonomy, thus threatening the ability to make autonomous choices.<sup>153</sup> Finally, the existence of such a multitude of risks within ToS and PPA, regardless of the content, constitutes a violation of user autonomy. Users' lack of knowledge regarding these various risks creates a situation in which users cannot provide free and informed consent to use the apps. As such, ToS and PPA may in fact work against their presumed purpose of protecting user rights. Instead, ToS and PPA often inherently increase the vulnerability of users, as they contain language that legalizes all ethical risks.

---

149. See Grafanaki, *supra* note 124.

150. See Cohen, *supra* note 120; Solove, *supra* note 144.

151. See Kosinski et al., *supra* note 122.

152. See Cohen, *supra* note 47; Tene & Polonetsky, *supra* note 120.

153. Susser et al., *supra* note 19, at 2–3, 6.

The discussion in previous sections demonstrated how four key pieces of legislation—the GDPR, the Consumer Rights Directive of the EU, the CCPA, and the CPRA—address the various risks presented. The Article focused on consumer protection and privacy protection legislation because users are likely to expect to find their rights with respect to ToS and PPA in these directly related legal instruments. My analysis of these laws vis-à-vis the typology of ethical risks in ToS and PPA suggests that standard practices and tools are still unable to meet the unprecedented challenges of the digital age. This inability to keep up with the digital age exists despite many regulatory advances in privacy protection and legislative attempts to align with technological developments and protect individual rights. The legislation reviewed does not cover the entirety of the laws that exist on these risks. However, the fact that there is no one clear legislative reference that can guide users in signing these everyday contracts is problematic.

All four laws are silent regarding several primary risks and secondary risks. There is no reference to the secondary risk of inability to condition over a specific clause; the secondary risk of content removal clause; the secondary risk of unilateral termination clause; and the secondary risk of unilateral changes of financial charges. Further, not one of these four laws address the primary risk of tracking user information and its secondary risk of tracking user activities while users are not using the app (via cookies).

In the CCPA—unlike the GDPR, which ascribes great importance to informed consent and processing user information—there is no specific direct reference to these main risks. Instead, the reference to these risks occurs indirectly, scattered throughout different sections. The CCPA is silent regarding a number of primary and secondary risks, including the primary risk of limited readability and its secondary risks: ambiguity, complexity, length, misleading or unclear language, and difficulty of navigation. and the secondary risks of processing user information, transforming meta-data into significant user information, and aggregating user information from multiple sources. In fact, the CCPA defines the term “aggregating user information” but does not refer to it beyond that. Additionally, the CCPA does not address the primary risk of profiling and its secondary risks: creation of user profiles that negatively affect future opportunities, personal information that may be used to discriminate, using profiles for undeclared purposes, and creation of aggregated profiles.

The CPRA extends the reference given to the term consent in CCPA. It defines the term “consent” and even refers to its secondary risks, such as the risk of broad purpose limitation, and the risk of inability to delete user account data. Unlike the CCPA, the CPRA addresses the risk of limited readability and states that specific sections must be clearly written to the average user. Also, the CPRA addresses the risk of profiling, defines what a profile is, and says that specific regulations dealing with the profile

should be established. In addition, with respect to the risk of personal data processing, the CPRA expands the reference to this risk and adds regulatory restrictions with respect to information processing. Regarding the risk of transferring information to third parties, the CPRA defines the term “information sharing” not previously defined in the CCPA. Despite the legislative progress made by the CPRA, especially regarding aspects of privacy and information protection, some risks still remain unaddressed, such as the secondary risk of transforming meta-data into significant user information and the secondary risk of aggregating user information.

While the GDPR places emphasis on informed consent, it does not refer to the risk of information transfer to third parties beyond a definition of this term. The reference in the GDPR to the issue of third parties primarily concerns the transfer between countries, and not between third parties in general or between subsidiaries. Also, the GDPR does not directly address the primary risk of limited readability and its secondary risks ambiguity, complexity, length, misleading or unclear language, and difficulty of navigation.

The European Consumer Protection Law does not address the primary risk of restricting user legal action or its secondary risks—mandatory arbitration, choice of law, choice of jurisdiction, and limitation of liability. Rather, it directs each state to act in accordance with the laws of the state, both regarding consumer protection and contract law.

The proposed typology indicates that the key laws in Europe and California that are supposed to address aspects of data, privacy, information protection, and consumer protection do not sufficiently address significant ethical risks in ToS and PPA of digital apps. If information regarding the grave risks presented in the typology will continue to be scattered across various pieces of legislation, users are unlikely to understand and exercise their rights. Including all relevant standards within one integrated legislative framework that is more accessible to lay consumers would be a worthy pursuit.

The typology rectifies the shortcomings of prior frameworks by taking a more holistic approach and drawing upon expert information from the field of law. Previous studies were more limited in that they detailed various ethical risks existing only in PPA of digital apps and were focused solely on deliberate learning purposes.<sup>154</sup> In these studies, researchers used machine learning techniques to map and categorize existing risks within privacy policies, so as to direct users’ attention to these risks. However, these initiatives are based on a risk typology developed by computer scientists, rather than jurists and content experts in the field. In addition, the studies addressed the various risks of a limited privacy breach, as reflected in the privacy policies of digital apps but did not address ToS of apps. Moreover, the studies mainly focused on the GDPR (rather than additional pieces of legislation), and very specific types of risks, including

---

154. See Kumar et al., *supra* note 2; Tesfay et al., *supra* note 2.

data collection, third-party sharing, data security, data aggregation, and control of data. These risks concern only information protection and information security aspects.

The Article expanded the existing framework and examined ethical risks in both ToS and PPA. It also addressed the vulnerability caused by these ethical risks in regard to core rights, including the right to autonomy, non-discrimination, freedom of expression, and consumer protection. Additionally, the typology includes details of each risk, how the risks are reflected within ToS and PPA, and the ways in which the various pieces of legislation address each risk, if at all. As demonstrated by the Article, it is not enough to examine the various risks in regard to only the limited aspect of privacy, as such a narrow examination does not allow for a complete solution to the various problems that exist in these legal tools. Additionally, an examination of risks that exist only under the GDPR is also very limited; as shown, the four laws reviewed are silent on many risks that exist in ToS and PPA. Expanding the ethical risks framework, and examining it within both ToS and PPA, is essential for finding an adequate solution to the infringement of user rights due to the use of digital apps.

#### CONCLUSION

This article sheds light on the gray areas of ToS and PPA of mobile apps—the ethical risks that characterize them. It presents a novel typology of issues hidden within these documents that are not necessarily prohibited by law, but nonetheless may significantly violate individual rights, such as the right to autonomy, privacy, non-discrimination, freedom of expression, consumer protection, and property. Scholars have long been concerned with identifying ethical risks in legal documents; however, they have tended to focus only on specific risk groups. The typology presented here creates a comprehensive framework for discussing and addressing the different ethical risks that are embedded in mobile app user agreements. This analysis enables, in turn, developing a comprehensive tool for risk analysis and for understanding the inter-relations between the risks. The analysis suggests that treating one ethical risk may result in a domino effect that affects (for better or worse) other risks.

The typology has implications for a variety of fields. For example, computer scientists can utilize it to develop tools that can more efficiently identify ethical risks; consumers can review the typology themselves to improve their understanding of ethical risks in ToS and PPA; and mobile app providers can refer to the typology to create more ethical agreements. On a broader level, the risks identified in the current typology can inform privacy protection and consumer protection regulatory efforts. Finally, researchers can use the typology as a framework for purposes such as evaluating user perceptions of ethical risks and gaining an understanding of how knowledge about the significant risks within ToS and PPA influences people's decisions about whether to use particular apps.

