

**Name:** Autumn Rains

**Date:** October 2, 2021

**Website Name:** Grubhub

**Website Privacy Policy:** <https://www.grubhub.com/legal/privacy-policy>

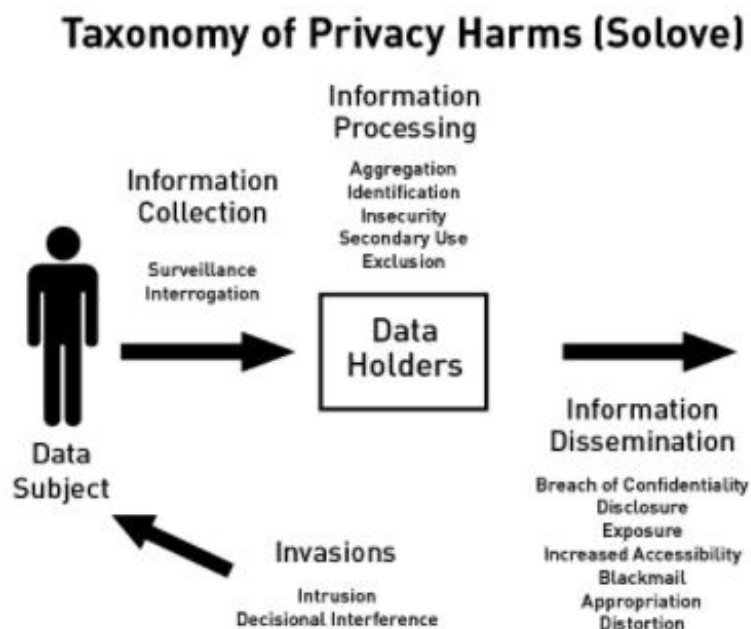
Additional Supplement - 'CA Privacy Notice': <https://www.grubhub.com/legal/ca-privacy-notice>

## Introduction

The online food delivery market has grown rapidly since the onset of the Covid-19 pandemic. According to research from McKinsey & Company, the growth rate doubled in the United States (Ahuja et al., 2021). One of the top four platforms for this service is Grubhub. According to their website, Grubhub serves over 33 million people with partnerships of over 300,000 restaurants in more than 4,000 U.S. cities. Grubhub achieves this through a web and mobile platform promising top-notch privacy for users. With that in mind, as we continue, we will explore how Grubhub's privacy policy, collection and use of personal information, and users' expectations of privacy intersect. We will explore the relationship of three perspectives (Solove's Taxonomy, Nissenbaum's Contextual Integrity, and Mulligan et al's analytic) to Grubhub's privacy proclamations. Additionally, Grubhub's policy will be reviewed through two frameworks pertaining to notice and consent: the Federal Trade Commission Principles from 2012 and The California Online Privacy Protection Act of 2003 (CALOPPA).

## Solove's Taxonomy of Privacy Harms

Dan Solove's Taxonomy casts privacy and violations as harms through the process of the full data lifecycle. For example, harms can include loss of control of an individual's data (dissemination) or the due process around data (opting in or out). Figure 1 below depicts the taxonomy in more detail.



**Figure 1:** Solove's Taxonomy Diagram, borrowed graciously from the W231 MIDS async materials. (W231 2021)

From Figure 1, there are several stages in the data lifecycle to introduce potential harms. Upon reviewing Grubhub's privacy policy, the structure of the policy follows the data lifecycle from initial collection through to storage for the use of the platform user interfaces (mobile or web) and service. The policy includes details of the collected information, how Grubhub intends to use it, how and when third parties may access this data, and ending with storage and dissemination information. However, there were two interesting details within the policy to further note.

The first interesting aspect pertains to customers using the platform who do not reside in the United States. The policy states that upon use of the site, even if the user is a resident of a country with specific data jurisdiction laws like the European Union, that the user agrees to the Grubhub policy. It also states that the information about the user 'may' be transferred to regions or countries where the jurisdiction does not apply. (*Note: This language can be found in the first section of Part 5: 'How We Store and Protect Your Information.'*)

The second interesting aspect is regarding the use of third-party services specific to 'Location Information.' Summarizing from the policy, Grubhub may use third parties to help with location identification through several methods collectively referenced as 'tracking technologies'. While these methods do not appear novel, the largest concern is found in the details of why it is collected. After stating general language around improving the platform service, the following statement is vague enough to cause concern:

"We, or the third-party partners we use, may use the data collected automatically through tracking technologies to: [...] (h) otherwise plan for and enhance our Services and **for other internal purposes.**" (*Note: This language can be found in the first section of Part 1.2: 'Location Services.'*)

This language does not give confidence that any individual's data is not being used for secondary purposes beyond my knowledge and/or consent. This would, in theory, violate the Solove Taxonomy if Grubhub was indeed using this data for additional research or design purposes not previously disclosed. However, the Grubhub policy has added a statement in Section 2 ('How We Use Your Personal Information') that says the following:

"Other purposes disclosed at the time of collection. From time to time, we may use personal information for a specific purpose not contemplated by this Privacy Policy. In such an event, we will specifically disclose that use to you." (*Note: This language can be found in the first section of Part 2.7: 'Other purposes disclosed.....'*)

It is very clear that this is a catch-all to protect Grubhub. It does not prioritize the user. As a user for several years, I can confidently state that I have never received notice of any additional uses with my current account.

Considering the language above, it is unclear how one would opt out of these additional uses or even the option to totally opt-out for any future uses beyond the policy. Additionally, I do not specifically see language about how to update incorrect account information. There is a general 'Contact Us' for any follow-up questions about the policy or your specific account. Therefore, I would recommend clear language about how to opt-out in full from future use be included on the policy page. As a direct user, I would also like to see a clear path to request my personal data information within my account.

In conclusion, the privacy policy does align with my expectations and context of use of the platform and service. There were two surprises within the language based on course learnings thus far pertaining to non-U.S. residents' data use and vague additional internal use of data not detailed in the policy. Overall, the policy is fairly clear to comprehend as compared to other legal policy documents with strong reference to legal language clauses and disclosures. It is evident that Grubhub strives to be transparent and I cannot find any direct violations according to Solove's Taxonomy.

### **Nissenbaum's Contextual Integrity**

Privacy, according to Diane Nissenbaum, is about maintaining integrity within an information sharing environment. This framework considers the appropriate flow of information between all parties in varying settings. Therefore, it relies on social or cultural norms and expectations of all parties involved to follow those informational flows. Privacy concerns arise and may be violated when actions fall out of bounds of these norms and expectations. From this lens, the Grubhub policy captures personal, financial, and location information within a 'normal' social context for processing transactions for meal delivery to customers.

The flow of the information would not be out of bounds as compared to similar competitor services or products. As a user, I do expect location data to be a part of the equation to deliver meals to me. However, as mentioned in the previous section, the ability to request and view this information within the user account is limited.

Thinking further about information flows from Nissenbaum's perspective, I do have concerns about third-party usage. The Grubhub policy states the following:

"Our websites and online Services may include links to third-party websites, plug-ins and applications. Except where we post, link to or expressly adopt or refer to this Privacy Policy, this Privacy Policy does not apply to, and we are not responsible for, any personal information practices of third-party websites and online services or the practices of other third parties. To learn about the personal information practices of third parties, please visit their respective privacy notices." (*Note: This language can be found in section 7: 'Third-Party Websites.'*)

While this would generally be considered 'normal' legal language for products from personal experience, in terms of personal user data, this is terrifying. From initial review, it is not clear who these additional parties are without in-depth knowledge of the platform. If a user wanted to contact these additional parties, the path to do so is limited at best. To improve this, Grubhub should have a clear and updated list of these parties available on the website or app.

### **Mulligan et al's Analytic**

The analytic from Mulligan et al is a tool that details multiple dimensions of privacy theoretically from legal and philosophical perspectives. It frames privacy from multiple viewpoints and environments to enable a congruent discussion among interested parties. The Grubhub privacy policy articulates an introduction to their policy as follows:

"This Privacy Policy explains how Grubhub Holdings Inc. and its subsidiaries and affiliates ("Grubhub, "we", "us" or "our") collect, use, disclose, and otherwise process personal information in connection with our Platform. Our Platform includes: (i) our websites, including related subdomains; (ii) our

mobile, tablet and other smart device applications; (iii) application program interfaces, (iv) in-store kiosks and other online services, and (iv) any other tools, technology and programs now or in the future; in each case, that reference this Privacy Policy” (*Note: This language is the first paragraph after the welcome statement.*)

From the above statement, the *target*, or that which privacy protects, is the personal information of users. The *temporal scale*, or time span for privacy application, is indefinite. Additionally, the policy covers the website and mobile applications as well as other interfaces and kiosks, which all belong to Grubhub. But what about the data of users and the importance of providing privacy? This is partially captured in a later section:

“We may use the personal information to maintain the safety and security of our Platform and Services. For example, we:

- Detect or prevent fraud, abuse or other harmful activities,
- Diagnose or fix technology problems,
- Conduct security investigations and risk assessments, and
- Improve and enforce our security measures.”

(*Note: This language can be found in section 2.2: Maintain the safety....*)

This language is one-sided in favor of Grubhub. It lacks acknowledgment that users expect privacy at the initial stages of account setup through ongoing use via security measures. Users expect Grubhub to safeguard personal data for the entirety of the data lifecycle. Furthermore, the policy is written in such a way that the *subject*, or who is protected by the policy, is actually Grubhub more so than customers. Additionally, the Mulligan framework defines *justification* as the motivation to provide privacy. From the above language, it can be interpreted that the motivation is to protect Grubhub from fraudulent activity or security breaches. There is little information about how Grubhub should respond in these instances if a breach were to occur.

These issues raise concerns personally based on learnings thus far from an ethics and privacy course at UC Berkeley (MIDS W231). It is recommended that Grubhub add language in the introduction of the policy to explain why privacy matters to them, but also why it is inherently expected from users. The users and their accompanying personal data are the basis of the platform. Grubhub should acknowledge this as much as possible.

### **FTC Principles (2012)**

The Federal Trade Commission (FTC) created privacy principles as a framework based on the 40-year history pertaining to consumer privacy in the form of policy and enforcement. There are three key principles:

1. Privacy by Design: Privacy should be incorporated in product development at every stage.
2. Simplified Choices for Businesses and Consumers: Decisions about data should be available to consumers. Businesses should have burden reduction through removing complex choices on data.
3. Greater Transparency: Any information collected and the use of such should be transparent.

Given the above policies, the Grubhub policy is moderately transparent. However, the decisions about consumer data are not that simple. To request such information and the ability to opt-out would require additional steps through directly communicating with the company. There are steps users can follow to opt-out of marketing emails through unsubscribing, but anything about personal data sharing or storage is not included. (*Privacy report - federal trade commission | protecting ... 2021*)

## CalOPPA

The California Online Privacy Protection Act of 2003 (CalOPPA) was a unique law requiring privacy policies for commercial websites and online services that collect personal information about residents of California. Highlights of this law can be seen in Figure 2 below [CALOPPA SOURCE]:

### HIGHLIGHTS OF RECOMMENDATIONS

#### Readability

- Use plain, straightforward language. Avoid technical or legal jargon.
- Use a format that makes the policy readable, such as a layered format.

#### Online Tracking/Do Not Track

- Make it easy for a consumer to find the section in which you describe your policy regarding online tracking by labeling it, for example: "How We Respond to Do Not Track Signals," "Online Tracking" or "California Do Not Track Disclosures."
- Describe how you respond to a browser's Do Not Track signal or to other such mechanisms. This is more transparent than linking to a "choice program."
- State whether other parties are or may be collecting personally identifiable information of consumers while they are on your site or service.

#### Data Use and Sharing

- Explain your uses of personally identifiable information beyond what is necessary for fulfilling a customer transaction or for the basic functionality of an online service.
- Whenever possible, provide a link to the privacy policies of third parties with whom you share personally identifiable information.

#### Individual Choice and Access

- Describe the choices a consumer has regarding the collection, use and sharing of his or her personal information.

#### Accountability

- Tell your customers whom they can contact with questions or concerns about your privacy policies and practices.

**Figure 2:** CALOPPA Highlights of Recommendations, page 2 of executive summary

Reading the Grubhub policy with regard to the CalOPPA, it has readability. Overall, the policy makes use of common language and does not exclusively include legal language that only experts could interpret. The general privacy policy does not include language around 'Do Not Track.' However, browsing the site further, an additional document pertaining to California was identified ('CA Privacy Notice'). This

document does have explicit sections on how to exercise an individual's right to know, delete and opt-out of the collection or sale of personal data, or request for deletion of personal data. Additionally, Grubhub has created a data portal to manage these requests, as shown below in Figure 3:

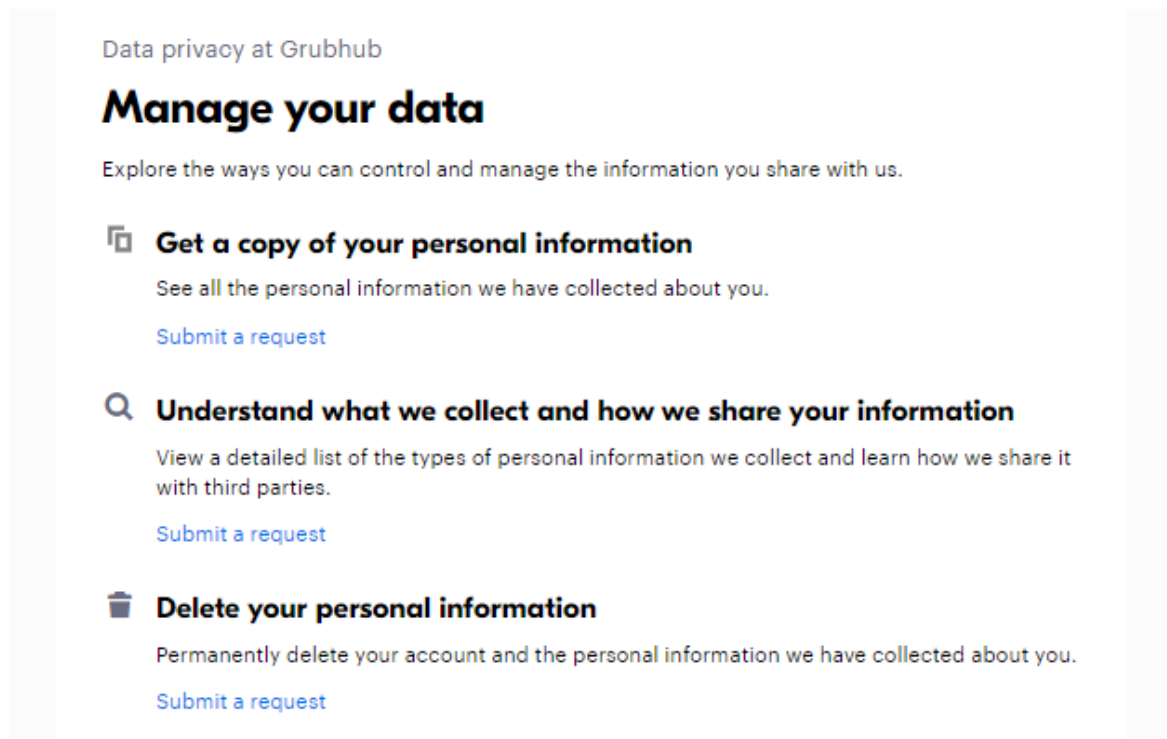


Figure 3: Grubhub Privacy portal

## Conclusion

Privacy is 'essentially contested,' as Professor Deirdre Mulligan, contributor to the Mulligan et al framework, profoundly articulates. Privacy can be defined through many lenses. The above discussion utilizes three frameworks and two principle sets to examine the privacy policy of Grubhub, an online food delivery service. As explored, there were areas where Grubhub complied with aspects of these frameworks, but there were also areas identified for improvement. Generally, Grubhub could make additional efforts to communicate about third-party sites or services and provide clearer access to users on how to review, edit, or delete personal data as desired. Grubhub does comply with current laws, but given the visibility to privacy and legal discussions at present, they would be wise to consider these improvements sooner rather than later.

## Addendum

At the time of submission of this writing assignment, I have personally reached out to Grubhub to request more information about the data on file for my account (as a resident of Colorado). I have not yet heard back from my initial query. Following upon my recommendations stated previously, I would encourage Grubhub to have a specific communication channel for these topics as well as a clearer way to explore my data on file as an active user for those individuals residing outside of California.

This has been an enlightening exercise!

## References

- Ahuja, K., Chandra, V., Lord, V., & Peens, C. (2021, September 23). *Ordering in: The rapid evolution of Food Delivery*. McKinsey & Company. Retrieved October 2, 2021, from <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/ordering-in-the-rapid-evolution-of-food-delivery>.
- Food delivery: Restaurant takeout: Order food online*. grubhub. (n.d.). Retrieved October 2, 2021, from <https://www.grubhub.com/legal/ca-privacy-notice>.
- Food delivery: Restaurant takeout: Order food online*. grubhub. (n.d.). Retrieved October 2, 2021, from <https://www.grubhub.com/legal/privacy-policy>.
- Making your privacy practices public - attorney general of ...* (n.d.). Retrieved October 2, 2021, from [https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making\\_your\\_privacy\\_practices\\_public.pdf](https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf).
- Privacy report - federal trade commission | protecting ...* (n.d.). Retrieved October 3, 2021, from <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.
- W231. Learn.datascience.berkeley.edu. (n.d.). Retrieved October 2, 2021, from <https://learn.datascience.berkeley.edu/>.