Assessing Instacart's Privacy Policy with Respect to Existing Frameworks

Author: Maria Auslander
Name of Service: Instacart
Link to Privacy Policy Statement: https://www.instacart.com/privacy

Introduction

Instacart's privacy policy treads a fine line between being informative and elusively vague. The policy briefly reviews the data collected about users through the use of Instacart and its affiliates in clear language, but refrains from providing concrete detail on information collection and dissemination. The following discussion assesses Instacart's privacy policy in terms of existing frameworks and brings to light areas of concern for Instacart users. Throughout the discourse, terms will be bolded as they pertain to existing privacy frameworks detailed by Solove, Nissenbaum, and Mulligan et al. Please see appendix A1 for details on term definitions and origins. The discussion will start with a dialogue around Instacart's privacy policy with respect to existing frameworks, follow with an assessment of the policy's adherence to FTC and CALOPPA regulations and suggestions, and will conclude with a discourse on user perceptions and expectations of the privacy policy.

Policy Discussion With Respect to Existing Frameworks

The **data subject** of interest in Instacart's privacy policy is an Instacart user. The user is subject to information collection through **surveillance** with the use of cookies which track user actions and through the use of **interrogation** when the user provides information necessary to order groceries through the application (i.e. address). Instacart acts as a **sender** and **recipient** of **subject** information--sending information to third parties and receiving information from third

parties in order to analyze user actions and potentially advertise or make other decisions based on the data analysis at hand.

When discussing the types of information (or **attributes**) that may be collected about a user, Instacart provides examples rather than an explicit list. The policy mentions the collection of personally identifiable information (PII) such as “name, email address, and zip or postal code”. However, data collection is not mentioned in definite terms, the policy prefaces the collection of information with terms such as “information like” as well as “information including”. The use of indefinite terms is also evident where the policy describes how information is used (“III. How We Use Your Information”) use cases “including” those listed are mentioned, indicating an non-exhaustive list. Vague terms are likely used so Instacart can more easily collect additional user data without having to specify each data point being collected; essentially using data for purposes beyond what is necessary for the application to function (**secondary use**). This may allow Instacart to participate in a type of **appropriation** where data is used in cases which benefit Instacart, but do not necessarily benefit the user; for example, the data may be used for advertising or for tracking user actions to inform future analysis and decision making.

The privacy policy provides the most clarity when detailing information collected when a user orders pharmaceuticals through the application, stating pharmacies “will not disclose to us the name, quantity, manufacturer or distributor of the prescription drug you have ordered or any other PHI about you other than your status as a patient of the pharmacy.” This additional specificity around **transmission principles** concerning Protected Health Information (PHI) is likely due to additional protections around PHI through the context of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). The policy has a separate section concerning PHI (“V. Personal Health Information”) which gives additional context and

justification around PHI information dissemination and protection practices; stating it will only be shared if it is necessary to provide services, it has been de-identified, there is written consent for sharing, disclosure is required by law, or Instacart is acquired or goes bankrupt.

While Instacart is an obvious data holder of sensitive user information, the privacy policy brings to light other third party data holders who may have access to user data. The policy states Instacart uses third parties to better understand how users interact with the application, using Google Analytics as an example, “we use Google Analytics to understand, in a non-personally identifying way, how users interact with various portions of the Services.” This indicates information is collected in a non-identifying way, however, it is not clear that employees or other parties associated with Instacart do not have access to tables which, when joined with other information, would be able to link data to a specific user. It should be noted the policy does not list all potential third parties who may receive user information, opening the floodgates for potential appropriation of data. Additionally, by sharing user information with third parties, Instacart may potentially be participating in a **breach of confidentiality** with its users.

In cases where a user is subjected to data collection and dissemination through many streams, he or she may want to be able to delete data or follow up on any data errors. In these cases, the policy claims account information can be “updated or corrected by accessing your account settings”, but does not specifically mention what information can be updated or corrected. The policy gives no indication as to a **temporal scale** or **quantitative scale** taken into account in housing user data; there is no indication past or incorrect data will be deleted and there is no indication as to the full scope of data being collected. The policy does not mention practices to uphold high data quality, a lack of data quality may lead to **distortion** of user information.

Concerning user choice around the user data being used by Instacart, the policy claims a user can adjust their browser settings to limit data collection through cookies and mentions the use of a “Do Not Track” signal which is available to users in some browsers. However, the policy states that because “there is no industry consensus as to what site and app operators should do with regard to these signals” Instacart does “not monitor or take action with respect to “Do Not Track” signals”. Unlike other statements in the privacy policy, this stands out as a blatant disregard for the preferences of users in terms of the collection and dissemination of their data. Instacart passes off responsibility to follow “Do Not Track” options to the law, stating, “Until the law is interpreted to require us to do so, we do not monitor or take action with respect to “Do Not Track” signals”.

The previous discussion has focused on intentional ways in which Instacart may collect, share, and use user information, but protecting against unwanted **invasions** where data is obtained by malicious actors **from-whom** information flows in non-conventional means is of additional importance. Instacart’s privacy policy has a section titled “Security” which gives brief detail on Instacart’s security practices. The policy states “reasonable” administrative, physical, and technical measures are used to protect subject information, but does not detail **mechanisms** used to secure user information or the **providers** who are charged with protecting data, only providing additional detail of security methods (encryption at rest and in transit) within the **social boundary** of PHI. This section houses another mention of law, letting the user know Instacart is legally required to notify users of any security breaches around their PHI or PII. Instacart tends to bring the law into the discourse of the policy where required (i.e. around PHI, PII, and the U.S. Children’s Online Privacy Protection Act, or “COPPA”).

Taking Into Account FTC and CALOPPA Suggestions and Principles

Instacart users would benefit if Instacart more clearly followed privacy suggestions provided by the Federal Trade Commission (FTC) and the California Online Privacy Protection Act (CALOPPA). Further discussion is below.

FTC Principles

The FTC laid out principles to protect consumer privacy in an internet-centric world in 2012, influenced by the Fair Information Practice Principles (FIPPs). The principles highlight privacy by design, simplified choice for businesses and consumers, and greater transparency. Based on their privacy policy, Instacart does not appear to follow these guidelines wholly.

The FTC suggests building products which invest in privacy at each stage of development. Instacart does not appear to have invested in consumer privacy at each stage of development, but rather when required. For example Instacart provides additional context around the collection and use of data with respect to PHI and to California residents, but these decisions appear to be largely influenced by regulations (HIPAA and CCPA respectively) rather than Instacart's opinion on how customers should be treated. An example of Instacart not valuing customer privacy is evident in how they target customer advertisements based on an analysis of specific customer data. In this case, users are not allowed to explicitly opt into this targeted advertising and analysis, but are rather forced to opt out of advertising. A better design would allow users to opt into targeted analysis and advertising.

The FTC suggests consumers are given a choice with regard to decisions about their data, and highlights the use of "Do Not Track" options consumers are able to select which provide simple decision points for businesses to use in terms of customer tracking. As previously stated, Instacart does not take into account "Do Not Track" options for users as there

is no clear law around these options, this represents a disregard for privacy and customer freedom around the treatment of their data.

Finally the FTC suggests greater transparency in consumer data practices, stating businesses should make data collection and use practices transparent. The privacy policy laid out by instacart lacks transparency. Users are not told which data fields specifically are collected about them and are not made aware of specific potential decisions that may be made based on analysis of their data rather than advertising. The policy would benefit from a comprehensive list of data fields which may potentially be collected about a user and the means by which information is collected. Because Instacart lacks a comprehensive list of potential consumer-related data fields which may be collected and used, it may be reasonable to assume the list of data fields Instacart uses and collects around consumers may vary by use case. There is a concerning amount of ambiguity in the privacy policy.

CALOPPA

Due to the CALOPPA, additional disclosures are required of commercial websites and online services to protect California residents. Instacart is tasked with adhering to CALOPPA as it operates within California. Instacart provides additional notice to California residents in its policy, however, this section is specified under the California Consumer Privacy Act of 2018 (CCPA) rather than CALOPPA. This section details the types of information Instcart collects with regard to CCPA (identifiers, other individual customer records, demographics, commercial information, internet activity, geolocation data, sensory information, nterences, and health information). The section also details how California consumers are able to “know and delete” data Instcart may have pertaining to specific users. Instacart gives the option to download personal information or request deletion of information in two ways, through a form or through an email. These methods seem reasonable.

While the section of the privacy policy concerning California residents does not specifically call out CALOPPA, it is evident Instacart has followed the suggestions of CALOPPA in crafting their privacy policy. CALOPPA suggests privacy policies are readable, that online tracking practices are taken into account, that data use and sharing is described, that the user has a choice regarding data collection, use, and sharing, and that there is accountability for customer privacy. Instcart takes into account the recommendations listed, but lists disappointing practices concerning "Do Not Track" user options and an individual's right to choose how his/her/they data is collected, used, and shared.

The policy is written in clear language (this opinion is corroborated with additional user opinions through user testing) and the format is reasonable and organized. With respect to data use and sharing, Instacart provides some detail on the information collected, but does not provide a comprehensive list of use cases for customer data in the document. The policy clearly states Instacart contact information at the end of the policy in order to uphold some accountability, giving multiple avenues of contact to the company (address, email address, phone number, help center application).

The areas where the policy is lacking when taking into account the CALOPPA are around "Do Not Track" options and an individual's right to control their data. The policy lays out how Instacart takes into account "Do Not Track" options are responded to, but mentions that due to a lack of regulations around "Do Not Track" options, they do not take the option into consideration, this is an obvious disregard of user preferences with regard to their personal data. It is likely not surprising Instacart tends to track user information without explicit consent to what specific data is being collected at points in time and without specific use cases for data laid out. This may be of particular concern to non-California residents who do not have the option to "Know and Delete" information collected about them through Instacart and its affiliates.

User Expectations of the Privacy Policy

To close this discussion, a review of user expectations and suggestions relating to Instacart's privacy policy will follow. As a user of Instacart, the policy detailed above is about in line with what I would expect of the application. The detailing of vague use cases rather than concrete, exclusive lists detailing all potential methods of data collection and dissemination makes sense as Instacart probably holds the wealth of information they're able to access about users in high regard.

While expected, the information detailed in the privacy policy does not fall short of disappointing. I would appreciate further detail in the privacy policy as to what data is being collected, how the data is being analyzed, and what decisions may be informed by the data analysis at hand. I think the area where the privacy policy was most lacking was the omission of detail on potential decisions that may be informed by user-specific data collection and analysis. If Instacart used customer data to profile users and treated customers in different, inequitable ways based on the data analysis, that would be concerning. Additionally, if Instacart shared potentially harmful information or analyses with third parties, there would be cause for additional concern. The privacy policy does not ensure analysis around user data will not lead to harm, intentionally or otherwise. The policy does not detail how potential harms to users may be mitigated other than in the case of PII or PHI data breaches, where the user will be informed. The policy does not give any detail as to potential mitigation or compensation if there is a data breach.

Beyond personal opinions around the privacy policy, additional responses to the policy were received through User Testing (See section A2 of the appendix). Users tended to believe the information presented in the privacy policy was sometimes vague, but appreciated that the

policy was written mainly in clear language. The users appreciated that the policy was concise. The users did not tend to oppose the use of third parties and cookies to track users in a way that led to targeted advertising, but were concerned about the treatment of the “Do Not Track” options users may select. The users believed the company should take “Do Not Track” options into consideration, regardless of the law. Overall, the users agreed the policy was standard and fulfilled their expectations of a privacy policy.

While the privacy policy was seen as standard to consumers, Instacart could improve their privacy policy and privacy practices to the benefit of their users. In order to better inform users of their practices, Instacart should better detail all potential avenues of subject data collection, data dissemination, and data security. Instacart should also provide concrete details into data analysis practices being used by the company and should inform users of any potential decisions which may be informed using data analysis driven by user data. Instacart should take user preferences on data collection into further consideration.

References

Harris, K. (2014, May). Making your Privacy Practices Public - State of California. Retrieved September 29, 2020, from https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

Leibowitz, J. (2012). *Protecting consumer privacy in an era of rapid change: Recommendations for business and policymakers*. Washington, DC: U.S. FTC.

Mulligan, D. K., Leibowitz, J. (2012). *Protecting consumer privacy in an era of rapid change: Recommendations for business and policymakers*. Washington, DC: U.S. FTC.

Koopman, C., & Doty, N. (2016). Privacy is an essentially contested concept: A multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 374*(2083), 20160118. doi:10.1098/rsta.2016.0118

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus, 140*(4), 32-48. doi:10.1162/daed_a_00113

Privacy Policy. (n.d.). Retrieved September 21, 2020, from https://www.instacart.com/privacy

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477. doi:10.2307/40041279

Appendix

A1: Definitions and Origins of Terms

The following table provides additional detail around terms used throughout the prior discussion. The terms have been taken from Solove's Taxonomy, Nissenbaum's Contextual Integrity, and Mulligan et al.'s analytic. References provided to these works are in the “references” section.

Term	**Definition**	**Origin**
Data Subject	The individual whose life is most directly affected by data-related activities	Solove
Surveillance	The watching, listening to, or recording of an individual’s activities	Solove
Interrogation	Various forms of questioning or probing for information	Solove
Aggregation	The combination of various pieces of data about a person.	Solove
Identification	Linking information to particular individuals.	Solove
Insecurity	Carelessness in protecting stored information from leaks and improper access	Solove
Secondary Use	The use of information collected for one purpose for a different purpose without the data subject’s consent	Solove
Exclusion	The failure to allow the data subject to know about the data that others have about her and participate in its handling and use.	Solove
Breach of confidentiality	Is breaking a promise to keep a person’s information confidential	Solove
Disclosure	The revelation of truthful information about a person that impacts the way others judge her character	Solove
Exposure	Revealing another’s nudity, grief, or bodily functions	Solove
Increased Accessibility	Amplifying the accessibility of information	Solove
Blackmail	The threat to disclose personal information	Solove

Term	Definition	Origin
Appropriation	The use of the data subject's identity to serve the aims and interests of another	Solove
Distortion	The dissemination of false or misleading information about individuals	Solove
Intrusion	Invasive acts that disturb one's tranquility or solitude	Solove
Decisional Interference	The government's incursion into the data subject's decisions regarding her private affairs	Solove
Actors	Subjects, senders, and recipients of data	Nissenbaum
Subject (Nissenbaum)	Individual who data/information is related to	Nissenbaum
Sender	Entity involved in the distribution of information	Nissenbaum
Recipient	Entity who receives subject information	Nissenbaum
Attributes	Types of information	Nissenbaum
Transmission Principles	Constraints under which information flows	Nissenbaum
Object	That which privacy provides to those protected, i.e. privacy provides protected agents with X	Mulligan
Justification	The motivation and basis for providing privacy, i.e. privacy is justified because of X	Mulligan
Contrast Concept	That which contrasts to privacy, i.e. that which is private is mutually exclusive with that which is X	Mulligan
Exemplar	The archetypal threat to this concept of privacy, i.e. privacy is violated by X	Mulligan
Target	That which privacy protects, i.e. privacy protects things of type X	Mulligan
Subject (Mulligan)	Actor(s) or entity(ies) protected by privacy, i.e. privacy protects agent X	Mulligan
Action	The act or behaviour that initiates or constitutes a privacy harm	Mulligan
Offender	Actor(s) violating privacy, i.e. privacy violated by agent X	Mulligan

Term	Definition	Origin
From-Whom	Actor(s) against-whom privacy is a protection, i.e. privacy provides protection against agent X	Mulligan
Mechanism	That which instrumentally secures privacy, i.e. the lock on her door protected her privacy	Mulligan
Provider	Actor(s) charged with securing privacy, i.e. the telecommunications provider was responsible for technically securing the privacy of her communications	Mulligan
Social Boundaries	That wherein privacy applies, i.e. privacy applies in domain, situation, field, or site X	Mulligan
Temporal Scale	The time span at which privacy applies, i.e. privacy applies for a span of X time	Mulligan
Quantitative Scope	Extent of application of privacy, i.e. privacy should be applied with a scope of X	Mulligan

A2: User Testing Summary

The following section details the questions asked of users regarding Instacart's privacy policy and gives a summary of user verbal responses. The users were given an introduction to the problem and asked to complete 10 tasks.

Introduction

The intent of this task is to evaluate a privacy policy. Please read the policy in its entirety and provide feedback according to the questions given.

Tasks

1. Before reading the privacy policy, please discuss the type of information you'd expect to see in a company privacy policy. How do you expect companies to treat your data?
2. Launch URL: https://www.instacart.com/privacy You have been taken to a new page. When you see the page, move on to the next step.
3. What are your opinions on the "Information you provide to us or allow others to provide to us" section of the document? What are your primary takeaways from reading that section? [Verbal Response]
4. What is your opinion on the "Cookies, Pixels, and Other Tracking Technologies" section of the document? (Under "Technical information about usage of the Services")? What is your opinion on how the company treats "Do Not Track" cookie options? [Verbal Response]
5. After reading the "Log information" section (Under "Technical information about usage of the Services"), would you be more likely to log out of the service when it is not in use? [Verbal Response]
6. After reading the "Interest-Based or Online Behavioral Advertising" section (Under "Technical information about usage of the Services"), do you believe allowing users to opt-in to advertising services or making users opt-out of behavioral advertising is appropriate? [Verbal Response]
7. What did you take away from the "How we use your information" section? [Verbal Response]
8. What did you take away from the "What we share" section? [Verbal Response]
9. What did you take away from the "Security" section? After reading this policy, do you believe your personal information would remain secure if you were to use this application? [Verbal Response]
10. Was there any information shared in the policy that surprised you? [Verbal Response]

User One:

1. Expect a minimum amount of data collected. Would expect data to be encrypted and anonymized.
2. Done

3. Appreciates the language used in the section, likes that it's written in basic English rather than using jargon. Thinks tracking location information is "dodgey" or suspicious. The "Information We Collect" session is reasonable.
4. Seems to believe the section on cookies is more vague than the first section. Thinks the company should take the initiative to respect the "Do Not Track" option, thinks current response is disappointing
5. Does not think the log information section is clear, after reading the section however, they would tend to log out of the application when not in use to stop tracking. The definition of "services" mentioned is not clear
6. This question was not clear to the user. Should've asked the question in a more clear way. In an ideal word, you would opt into advertising rather than opt in, but they do believe an "opt out" model is appropriate considering the context.
7. This section is very vague and unclear. Assumes that Instacart is creating analysis on its users.
8. The user thinks the principles are outlined more clearly in this section. The external processing section is vague. Overall the points seem reasonable in context.
9. User is from outside of the US, but believes the language does not instill a great deal of confidence. Believes every service has a data breach risk, would not trust security wholly
10. Was interested in the additional regulations around PHI, overall thought the document was probably pretty standard

User Two:

1. Before reading the privacy policy, the user expected to gain knowledge on how the company treated user PII, the user expected to learn information about the company's data security practices
2. Done.
3. The user believed this section provided detailed information on how customer information is collected, and appreciated the examples. The user thought the language used in the statement was clear. The user omitted to not typically reading privacy policies
4. The user was not opposed to advertisements being targeted to him based on an analysis of his online services. He prefers targeted advertisements rather than random ones. The user appreciates transparency around the "Do Not Track" options that the policy provides, but would typically expect companies to adhere to a "Do Not Track" option provided by the user
5. User does not believe the risk is that high of staying logged on to the site, but is "50/50" on whether he would be more likely to log out of the website or not based on reading the "log information" statement
6. The user believes targeted online advertising is appropriate, he trusts the system. He said privacy may be more of a concern for high profile individuals or those who stand to lose more if their privacy is compromised

7. This section seems standard to the user, the user appreciates the transparency and how the statements are clearly laid out in bullet points. However the user believes there should be a link readily available in the policy for a user to opt out of certain advertising
8. The user does not have a concern with this section, he believes the company has been transparent through the language in this section (“What We Share” section)
9. The user believes the company is handling PII securely
10. The policy seemed standard to the user, the user appreciated the clear language and lack of legal jargon in the policy.

User Three:

1. The user would look at use cases for user data, the user wants to know what information would be used and if the data would be shared with third parties. The user would expect that the company adheres to laws based on the countries the company is operating in or out of (i.e. GDPR for Europe)
2. Done.
3. The user appreciated the simple language of the first paragraph. The user appreciated knowing why certain pieces of information were collected (i.e. age of user to purchase alcohol). The user appreciated additional detail around pharmaceutical information. The user appreciated knowing what information was shared between companies and thought this was laid out clearly. The last paragraph was unclear to the user in this section, it was not clear how/why/when user data would be used. The use of the “widget” made the language less clear in the final paragraph.
4. The user appreciated the brief explanation on what cookies are and how they’re collected and used. The user does not like that the company does not take into account “Do Not Track” options provided by the user, the language used is also seen as misleading (using “monitor” as term was seen as intentionally misleading)
5. The user does not see an issue with staying logged into the services, as long as the actions being tracked are only of relevance to the service itself and other online actions are not being tracked
6. The user believes this section is clear, the user liked that the link for opt out is directly in the policy. The user prefers targeted advertising.
7. The user thinks this section is clearly laid out and fulfills their initial expectations of a privacy policy. The user appreciates the clear language and the use of bullet points
8. The user thought this section was clear and transparent
9. The user did not understand “PHI” and thought the acronym should’ve been in long form first. The user would feel fairly confident in the security of their information. They appreciate knowing they will be notified of a data breach.
10. The privacy policy was as expected for the user. The user appreciated the clear language, but was disappointed in the “Do Not Track” section of the policy