



《第69回》プライバシーにおける使いやすさと向き合う

井手 絢 絵

1. はじめに

私は、現在米国大学院の情報科学博士課程に在籍し、プライバシーの研究に携わっています。これまでは、日本で修士を取得後、国内外のソーシャルメディアプラットフォームの企業にて分析職としてモバイルアプリの設計やオンライン広告の効果計測に取り組んできました。膨大なデータを取得するサービスに携わる中で、データ許諾の重要性とそのプロセスにおける体験設計の難しさに直面しました。たとえば、2021年にApple社が施行したトラッキング規制 App Tracking Transparency は、オンライン広告におけるプライバシー強化の流れを加速しました。この変更により、iOS アプリではデータ追跡許諾の表示が義務化され、暗黙的なデータ追跡が回避された一方で、ユーザ側の意思決定の負荷の増加や、関連性の低い広告が配信されることによる体験の質の低下が懸念されました。推薦システムをはじめとする個人データの活用が進む一方で、ユーザがデータ収集の実用性とリスクを理解し、適切に選択するための情報や機会はいまだ改善の余地があります。このような動機から、ユーザブルプライバシーの研究を志しました。

2. ユーザブルプライバシー

前述したユーザブルプライバシーという研究領域は、プライバシー研究の中でも人間の認知・心理的な側面や行動特性に焦点を当て、セキュリティやプライバシーの向上につながるシステムの設計をゴールとしています。代表的な研究トピックとしては、自然言語処理によるプライバシーポリシーの情報抽出の半自動化や、プライバシーの嗜好性予測など、プライバシーに関する意思決定を支援することを目的とした基礎研究や技術開発が含まれます。その点において、プライバシー領域に閉じず、心理学や工学など幅広い分野の専門家が交わる学際的な分野であり、調査方法も定量調査に限らずインタビュー

やエスノグラフィーといった質的研究がなされています。近年では、ユビキタスコンピューティングやスマートホーム、大規模言語モデル (LLM) などのトピックにも拡大すると同時に、社会動向を反映した包括性 (視覚障害をもつオンラインユーザのプライバシー¹⁾) や多様性 (LGBTQ+ や若年層などハラスメントの危険に晒されたグループの視点を反映した有害コンテンツのフィルタリング²⁾) に関する研究も注目を集めています。

3. 栄養成分表示とプライバシー

ここで、食品のパッケージに掲載されている栄養成分表示³⁾について触れたいと思います。栄養成分表示は各国の規制に基づいて標準化されており、表記方法や内容は統一されています。これにより、私たちは迷うことなく即座にカロリーや栄養バランスを確認することができます。一見すると無関係に思える栄養成分表示ですが、実はプライバシー文脈でのインタフェースの発展に寄与しています。Carnegie Mellon University と Microsoft の Trust User Experience チームらは、既存のプライバシーポリシーの難解な記述とユーザの理解のギャップに対処するため、栄養成分表示の枠組みを取り入れた情報設計によるプライバシー栄養ラベルを提案しました⁴⁾。彼らの研究は、プライバシーの情報設計において分野を牽引し、その醸成が反映された結果、2020年にAppleはプライバシーポリシーの内容を標準化し、簡易的にラベルとして表示するプライバシーラベルをApp Storeに導入しています⁵⁾ (図1)。誰もが馴染みのある身の回りのデザインから着想を得ることで、ユーザの認知負荷を削減し、食品を買う際に栄養表示を確認するような手軽さで、アプリを使う際のプライバシー管理ができるようなインタフェースの実現に近づいています。

4. 差分プライバシーの個人化に向けて

博士課程の1年目では、差分プライバシー (Differen-

Nutrition Facts	
16 servings per container	
Serving size 1 Tbsp. (21g)	
Amount per serving	
Calories	60
% Daily Values*	
Total Fat 0g	0%
Saturated Fat 0g	0%
Trans Fat 0g	
Cholesterol 0mg	0%
Sodium 0mg	0%
Total Carbohydrate 17g	6%
Dietary Fiber 0g	0%
Total Sugars 17g	
	34%
Protein 0g	
Vitamin D 0mcg	0%
Calcium 0mg	0%
Iron 0mg	0%
Potassium 0mg	0%

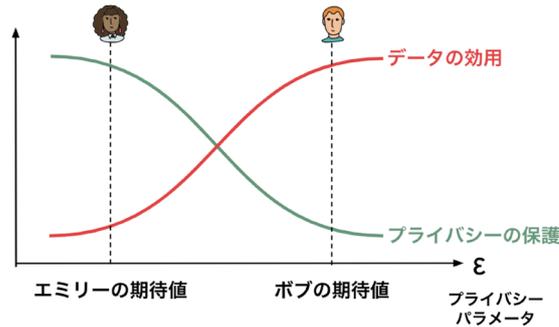
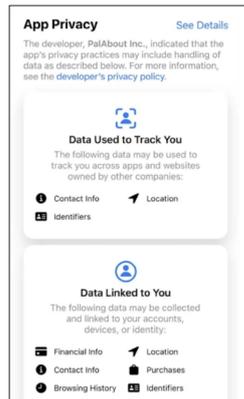


図 2 個人のプライバシー嗜好性の違い

図 1 米国 FDA 栄養成分表示 (左) と Apple の Privacy Nutrition Label (右)

tial Privacy (DP)) の情報設計並びにプライバシーの嗜好性把握に関する研究プロジェクトに取り組みました。DP は、数理的なパラメータで制御されたノイズをデータに付与することで、個人識別を困難にしながデータの有用性を維持するプライバシー保護技術の一つです。DP のプライバシーパラメータ ϵ は、プライバシー保護とデータ効用のトレードオフを決定づけるものであり、従来の DP では全ユーザに同一の値が適用されてきました。しかし、ユーザのプライバシーの期待値は一律ではなく、個人の嗜好性、さらには文脈的な状況やデータの機密性によって異なることを背景に (図 2)、個人のプライバシーの期待値に合わせてパラメータ選択を可能にするパーソナライズされた DP が提案されています⁶⁾。これは将来的にユーザ自身で自分の状況に適したパラメータを選択できることを意味し、データの実用性とリスクを考慮しながら適切な値を選択する必要があります。われわれの研究では、DP におけるプライバシーとデータ効用のトレードオフをユーザの文脈で説明し、パラメータの嗜好性にどのような個人特性が観察されるか、意思決定に影響する環境要因は何かを調査しています。

5. 米国博士課程のプログラム

私の所属する学科である IST (Information Sciences and Technology) は、4つの研究領域 Data Science& Artificial Intelligence (DS&AI), Privacy&Security (P&S), Human-Computer Interaction (HCI), Social& Organizational Informatics (SOI) をカバーしています。博士課程 1 年目は、この中から 3 つの分野の必修授業を履修する必要があります。学生は自身の研究内容に直結する分野だけでなく、関連する分野の基礎知識の習得を期待されます。私自身、プライバシーと HCI の中間に位置するような研究内容であるため、このような学際的な環境を推奨されている点は非常に有り難く、P&S の必修に加え、前期は HCI から人間中心設計、後期は SOI から質的研究の授業を履修しました。授業内のプ

ロジェクトでは必然的に他分野の学生と連携する機会が多く、お互いの専門性を共有できる点も良かったです。私のように社会人経験を経て博士課程に進学した同期も数多く、キャリアの多様性も居心地良く感じています。今後は、ユーザブルプライバシーに軸足を置きながら、分散型システムのアクセシビリティにも貢献したいと考えています。

(2024 年 6 月 11 日受付)

参考文献

- 1) D. Napoli, K. Baig, S. Maqsood, and S. Chiasson: "I'm Literally Just Hoping This Will Work:" Obstacles Blocking the Online Security and Privacy of Users with Visual Disabilities, In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 263/280 (2021)
- 2) D. Kumar, P. G. Kelley, S. Consolvo, J. Mason, E. Bursztein, Z. Durumeric, ... and M. Bailey: Designing Toxic Content Classification for a Diversity of Perspectives, In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, 299/318 (2021)
- 3) U.S. FDA, The Nutrition Facts Label, <https://www.fda.gov/food/nutrition-education-resources-materials/nutrition-facts-label>
- 4) P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder: A "Nutrition Label" for Privacy, In *Proceedings of the 5th Symposium on Usable Privacy and Security*, 1/12 (2009)
- 5) T. Li, K. Reiman, Y. Agarwal, L. F. Cranor, and J. I. Hong: Understanding Challenges for Developers to Create Accurate Privacy Nutrition Labels, In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1/24 (2022)
- 6) F. Boenisch, C. Mühl, A. Dziedzic, R. Rinberg, and N. Papernot: Have It Your Way: Individualized Privacy Assignment for DP-SGD, *Advances in Neural Information Processing Systems*, 36 (2024)

[著者紹介]

井手 絢 絵 君

2018 年東京工業大学情報理工学院修士課程修了。LINE, Meta を経て、2023 年 8 月よりペンシルバニア州立大学情報科学博士課程に進学。プライバシー・サイバーセキュリティ分野のユーザビリティ研究に従事。

E-mail: ayaeide@psu.edu

所属: The Pennsylvania State University, College of Information Sciences and Technology, Westgate Building, University Park, PA 16802, United States