Examining (In)consistencies in Privacy Disclosures and Controls in Fintech: The Limits of "Informed Consent"

LU XIAN, University of Michigan, USA
VAN TRAN, University of Chicago, USA
LAUREN LEE, University of Michigan, USA
MEERA KUMAR, University of Michigan, USA
YICHEN ZHANG, University of Michigan, USA
FLORIAN SCHAUB, University of Michigan, USA

ACM Reference Format:
Lu Xian, Van Tran, Lauren Lee, Meera Kumar, Yichen Zhang, and Florian Schaub. 2025. Examining (In)consistencies in Privacy Disclosures and Controls in Fintech: The Limits of "Informed Consent". In *Proceedings of Proceedings of CHI 2025 Workshop on the Future of Money and HCI (CHIworkshops'25).* ACM, New York, NY, USA, 4 pages.

1 EXTENDED ABSTRACT

As financial technologies increasingly rely on consumer data to deliver services, consumers' willingness and decision to share their data becomes critical. While digitization and technological advancements make it possible to use more diverse data sources to improve consumer experience and provide customized services [15], new forms of data collection and sharing pose privacy and security risks for consumers including but not limited to data breaches, security attacks, and data misuse [14, 16, 18]. To protect consumer privacy, existing privacy regulations rely on the "notice and choice" framework and require businesses to disclose their data practices in privacy notices and provide consumers with details on how to opt out of certain data practices [9]. While this framework is intended to empower consumers to make informed privacy decisions, it often falls short in effectively informing consumers and facilitating their ability to express choices [5]. To empower consumers, financial regulators are adopting new approaches like open banking and open finance policies that facilitate the secure sharing of account data with licensed third parties through Application Programming Interfaces. The secure data-sharing mechanisms enable customers to exercise control over their data, specifically authorizing third-party access to their information that banks have. However, the effectiveness of these approaches similarly relies on consumers' informed consent [22]—in order for consumers to understand the implications of their data-sharing decisions and data access permissions, consumers need to understand the financial institutions' data practices like how their data will be processed and analyzed, and if their data will be combined with other data

Authors' addresses: Lu Xian, xianl@umich.edu, University of Michigan, Ann Arbor, MI, USA; Van Tran, tranv@uchicago.edu, University of Chicago, Chicago, IL, USA; Lauren Lee, laurnlee@umich.edu, University of Michigan, Ann Arbor, MI, USA; Meera Kumar, meerakmr@umich.edu, University of Michigan, Ann Arbor, MI, USA; Yichen Zhang, zhyichen@umich.edu, University of Michigan, Ann Arbor, MI, USA; Florian Schaub, fschaub@umich.edu, University of Michigan, Ann Arbor, MI, USA.

Manuscript submitted to ACM

[4, 20]. Under the current regulatory framework, such information is provided in privacy notices, and the usability and usefulness challenges of the “notice and consent" framework remain.

Furthermore, nowadays businesses often have to comply with a range of notice and choice requirements, resulting in them providing multiple privacy notices. In the US, all financial institutions are subject to the federal Gramm-Leach-Bliley Act (GLBA), which governs how financial institutions use, share, and protect consumers' financial information. Banks are also subject to state-level privacy laws like the California Consumer Privacy Act (CCPA), if they do business in the respective state and meet certain criteria. Banks may provide additional privacy notices to be transparent about their website and app data practices as required by the Federal Trade Commission [10].

These privacy regulations have different requirements for privacy documents. The GLBA defines personally identifiable information (PII) narrowly as those relating to financial products or services [8]. In compliance with GLBA, the notices highlight data-sharing practices with affiliates and nonaffiliates for marketing purposes, for which opt-outs are required. Typically, these notices follow a standardized, table-based format, adhering to a two-page model privacy form [8]. In contrast, the CCPA defines PII more broadly as any data that identifies, relates to, or can reasonably be connected to consumers or their households. The CCPA requires businesses to provide details on whether PII is sold or shared with third parties and an explanation of consumers' right to opt out of sale/sharing of personal information. The notices are often presented in free-form text with varying structure, and at different locations across the websites, as CCPA does not prescribe a strict format. Banks may also have dedicated online, mobile, or cookie notices. Compared to GLBA and CCPA, these additional notices generally have fewer specific content requirements and thus vary widely in content, structure, and format. This proliferation of privacy documents requires consumers to find, read, and navigate multiple privacy notices and opt-outs provided by the same entity. Moreover, discrepancies among notices may mislead consumers and prevent them from making informed privacy decisions and fully exercising their privacy choices. In this study, we examine the (in)consistencies across privacy documents and opt-out choices provided by the same bank, i.e., inconsistencies in the implementation of different privacy regulations that a single bank is subject to.

We engage with three strands of prior work on privacy notices and controls. First, existing work has uncovered significant inconsistencies and contradictions in businesses' privacy disclosures and practices. These include inconsistencies in the stated collection and sharing practices within a privacy policy [1, 6], between the data-sharing disclosures and the availability of corresponding opt-out choices [24], and between privacy notices and actual data handling [2, 27]. These findings underscore that misleading privacy disclosures and non-compliant data practices are a recurring pattern that could undermine the transparency goals of privacy notices and erode consumer trust. Building on prior work that mostly studied specific and separate notices like the GLBA or online notices, our work takes a consumer perspective and analyzes multiple privacy notices and opt-out choices provided by the same institution.

Second, focusing on privacy notices' role in informing consumers about businesses' data practices, extensive research has examined the lack of readability of notices. For example, Chen et al.'s [3] analysis of the privacy policies of 95 popular websites found that despite the CCPA's mandate for clear privacy disclosures, businesses still vary significantly in both the level of detail provided in their privacy policies and their interpretation of key CCPA definitions. These inconsistencies directly impact consumers' ability to assess businesses' data practices. Similarly, in examining the impact of the GDPR on privacy disclosures, Kretschmer et al. [17] and Degeling et al. [7] found that while transparency has improved over time, usability challenges persist, particularly in the form of complex interface designs that restrict user agency. These findings suggest that despite regulatory intentions for transparency, the real-world implementations of them in privacy notices often remain too complex, inconsistent, or difficult to navigate, which limits their effectiveness

in truly informing consumers. In our work, we center consumers' information needs on exercising privacy controls and focus on the statements of data-sharing practices and opt-out choices across privacy notices.

Third, prior work highlighted that the design of privacy controls significantly affects consumer understanding and willingness to exercise their rights [11, 13, 23]. Standardized, visible banners improve opt-out rates and user satisfaction [23], while dark patterns can drastically increase the likelihood of users, especially those less educated, choosing less privacy-protective settings [19]. Despite their importance, privacy controls often present significant usability barriers [26]. Users frequently struggle to locate, understand, and effectively use these controls due to inconsistent placement, complex navigation, and a lack of clear instructions [12]. Studies have shown that dark patterns in consent pop-ups [21, 26] and CCPA opt-out processes [25] often make privacy choices less accessible or more confusing. These findings suggest poor usability and manipulative design of privacy controls are prevalent and undermine their intended purpose, making it more difficult for consumers to take control of their personal data. Our work collects a range of data-sharing privacy controls provided under different privacy regulations that consumers can exercise for a given institution, which lays the groundwork for a centralized design of privacy controls.

We collected the GLBA, CCPA, and online and mobile privacy notices and respective privacy controls for over 2,000 major banks in the US. We used quantitative methods (e.g., scraping, LLMs) to collect and analyze privacy documents and controls, and qualitative methods (e.g., inductive coding) to identify inconsistencies. On average, banks provide two privacy documents, typically GLBA and online notices, and yet some offer as many as five different notices. We found that (1) while the GLBA model notice is purposefully short, consumers now have to also consider additional CCPA and website/app notices, undermining the intended purpose of its concise format. (2) While many notices appear consistent, and are referenced in the GLBA notice, we identified some substantial discrepancies within the same institution—for example, a GLBA notice may state that data is not shared or sold to third parties, yet the same bank offers a do-not-sell opt-out under the CCPA. (3) The do-not-sell and cookie opt-outs are sometimes grouped together in the same banner without clear explanations, which may hinder consumers from understanding and exercising their choices.

Our findings demonstrate that the proliferation of notice requirements at the federal and state levels has led to a confusing mix of privacy notices in the US financial industry. Furthermore, the discrepancies within privacy documents and across privacy documents provided by the same institution suggest the need to harmonize notice and choice requirements across federal and state privacy and consumer protection laws to support consumers to make informed decisions about privacy in their interaction with financial technologies.

REFERENCES

[1] Benjamin Andow, Samin Yaseer Mahmud, Wenyu Wang, Justin Whitaker, William Enck, Bradley Reaves, Kapil Singh, and Tao Xie. 2019. {PolicyLint}: Investigating Internal Privacy Policy Contradictions on Google Play. 585–602. https://www.usenix.org/conference/usenixsecurity19/presentation/andow

[2] Muhammad Abu Bakar Aziz and Christo Wilson. 2024. Johnny Still Can't Opt-out: Assessing the IAB CCPA Compliance Framework. *Proceedings on Privacy Enhancing Technologies* (2024).

[3] Rex Chen, Fei Fang, Thomas Norton, Aleecia M McDonald, and Norman Sadeh. 2021. Fighting the fog: Evaluating the clarity of privacy disclosures in the age of ccpa. In *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. 73–102.

[4] Andy Crabtree and Richard Mortier. 2015. Human Data Interaction: Historical Lessons from Social Studies and CSCW. In *ECSCW 2015: Proceedings of the 14th European Conference on Computer Supported Cooperative Work, 19-23 September 2015, Oslo, Norway*, Nina Boulus-Rødje, Gunnar Ellingsen, Tone Bratteteig, Margunn Aanestad, and Pernille Bjørn (Eds.). Springer International Publishing, Cham, 3–21. https://doi.org/10.1007/978-3-319-20499-4_1

[5] Lorrie Faith Cranor. 2012. Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications and High Technology Law* 10 (2012), 273.

[6] Lorrie Faith Cranor, Pedro Giovanni Leon, and Blase Ur. 2016. A Large-Scale Evaluation of U.S. Financial Institutions' Standardized Privacy Notices. *ACM Transactions on the Web* 10, 3 (2016), 1–33.

[7] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096* (2018).

[8] Federal Trade Commission. 2002. How to Comply with the Privacy of Consumer Financial Information Rule under the Gramm-Leach-Bliley Act. Retrieved January 26, 2025, from https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act#whois.

[9] Federal Trade Commission. 2008. Fair Information Practice Principles. Retrieved January 26, 2025, from https://www.ftc.gov/fair-information-practice-principles.

[10] Federal Trade Commission. 2013. Marketing Your Mobile App: Get It Right from the Start. Retrieved January 26, 2025, from https://www.ftc.gov/business-guidance/resources/marketing-your-mobile-app-get-it-right-start.

[11] Hana Habib, Sarah Pearman, Jiamin Wang, Yixin Zou, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2020. " It's a scavenger hunt": Usability of Websites' Opt-Out and Data Deletion Choices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–12.

[12] Hana Habib, Yixin Zou, Aditi Jannu, Neha Sridhar, Chelse Swoopes, Alessandro Acquisti, Lorrie Faith Cranor, Norman Sadeh, and Florian Schaub. 2019. An empirical analysis of data deletion and {Opt-Out} choices on 150 websites. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. 387–406.

[13] Hana Habib, Yixin Zou, Yaxing Yao, Alessandro Acquisti, Lorrie Cranor, Joel Reidenberg, Norman Sadeh, and Florian Schaub. 2021. Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–25.

[14] Zhiguo He, Jing Huang, and Jidong Zhou. 2023. Open banking: Credit market competition when borrowers own the data. *Journal of Financial Economics* 147, 2 (Feb. 2023), 449–474. https://doi.org/10.1016/j.jfineco.2022.12.003

[15] Srihari Hulikal Muralidhar, Claus Bossen, Apurv Mehra, and Jacki O'Neill. 2018. Digitizing Monetary Ecologies: Intended and Unintended Consequences of Introducing a Financial Management App in a Low-Resource Setting. *Proc. ACM Hum.-Comput. Interact.* 2, CSCW (Nov. 2018), 72:1–72:17. https://doi.org/10.1145/3274341

[16] Paul Klumpes. 2023. Coordination of cybersecurity risk management in the U.K. insurance sector. *The Geneva Papers on Risk and Insurance. Issues and Practice* 48, 2 (2023), 332–371. https://doi.org/10.1057/s41288-023-00287-9

[17] Michael Kretschmer, Jan Pennekamp, and Klaus Wehrle. 2021. Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)* 15, 4 (2021), 1–42.

[18] Michele Loi, Christian Hauser, and Markus Christen. 2022. Highway to (Digital) Surveillance: When Are Clients Coerced to Share Their Data with Insurers? *Journal of Business Ethics* 175, 1 (Jan. 2022), 7–19. https://doi.org/10.1007/s10551-020-04668-1

[19] Jamie Luguri and Lior Jacob Strahilevitz. 2021. Shining a light on dark patterns. *Journal of Legal Analysis* 13, 1 (2021), 43–109.

[20] Helen Nissenbaum. 2011. A Contextual Approach to Privacy Online. *Daedalus* 140, 4 (Oct. 2011), 32–48. https://doi.org/10.1162/DAED_a_00113

[21] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. 2020. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376321

[22] Anshu Premchand and Anurag Choudhry. 2018. Open Banking APIs for Transformation in Banking. In *2018 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. 25–29. https://doi.org/10.1109/IC3IoT.2018.8668107

[23] Aden Siebel and Eleanor Birrell. 2022. The Impact of Visibility on the Right to Opt-out of Sale under CCPA. *arXiv preprint arXiv:2206.10545* (2022).

[24] Van Hong Tran, Aarushi Mehrotra, Marshini Chetty, Nick Feamster, Jens Frankenreiter, and Lior Strahilevitz. 2024. Measuring Compliance with the California Consumer Privacy Act Over Space and Time. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*. 1–19.

[25] Van Hong Tran, Aarushi Mehrotra, Ranya Sharma, Marshini Chetty, Nick Feamster, Jens Frankenreiter, and Lior Strahilevitz. 2024. Dark Patterns in the Opt-Out Process and Compliance with the California Consumer Privacy Act (CCPA). *arXiv preprint arXiv:2409.09222* (2024).

[26] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. 2019. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 973–990. https://doi.org/10.1145/3319535.3354212

[27] Sebastian Zimmeck, Oliver Wang, Kuba Alicki, Jocelyn Wang, and Sophie Eng. 2023. Usability and enforceability of global privacy control. *Proceedings on Privacy Enhancing Technologies* 2023, 2 (2023).