CENTER FOR INFORMATION TECHNOLOGY POLICY
PRINCETON UNIVERSITY

November 21, 2022

Via Regulations.gov
Before the
Federal Trade Commission
Washington, D.C.

Commercial Surveillance ANPR R111004

We appreciate the opportunity to aid the Commission's consideration of appropriate rules to govern the collection and use of personal data by commercial enterprises. We are interdisciplinary academic researchers associated with Princeton's Center for Information Technology Policy who study security and privacy practices of online platforms.[1]

Collecting and monetizing consumer data is a critical element of the business plan for many online platforms. We commend the Commission for initiating a formal public consultation to help determine what mechanisms are important to protect consumers from what the Commission terms "commercial surveillance."[2] From the Commission's list of 99 initial questions, we focus on a few below. We look forward to further opportunities to provide more detailed feedback on the proposed rules as they are developed.

[1] This Comment is the product of Princeton CITP's Technology Policy Clinic, which provides nonpartisan research, analysis, and commentary to policy makers, industry participants, journalists, and the public. The Comment reflects the independent views of the undersigned scholars.
[2] Defined by the Commission as "the collection, aggregation, analysis, retention, transfer, or monetization of consumer data and the direct derivatives of that information."

Our comment makes two recommendations to assist the Commission in designing rules to mitigate widely prevalent security and privacy failures. *First*, all companies should be required to adopt robust security measures to protect consumers. Many of these security measures are not that expensive to implement and are accessible to most small to medium sized businesses. *Second*, the Commission should support building effective mechanisms for public oversight of automated decision making systems because research shows that these systems are prone to errors and can cause significant harm, especially to vulnerable communities. Moreover, relying on a broken notice & consent framework to fix all problems that may arise from the use of such systems is plainly insufficient. The Commission should consider requiring substantive protections for consumers by default.

I. Widespread security vulnerabilities harm consumers and can be mitigated through cost-effective risk management strategies that can be tailored to differently situated businesses. (Questions 6 & 31.)

A. Non-pecuniary harms

There are a host of non-pecuniary harms that result from lax security practices that are often poorly accounted for despite exacting a serious toll. Such harms include physical, mental, relational, and reputational injuries when, for example, information is stolen or used to commit identity theft. While nationally

representative data on the impacts of data breaches and identity theft remains scarce, a few studies offer suggestive evidence about the scale of these different harms.

In the Department of Justice's 2016 survey of identity theft victims, for instance, 79% of the estimated 26 million victims nationwide reported experiencing at least some emotional distress resulting from their case, with 10% describing that distress as severe.[3] 2% of victims reported "significant problems with family members or friends," with that figure rising above 8% for individuals experiencing more severe types of identity theft.[4]

More recently, in a survey conducted by the Identity Theft Resource Center, 66% of identity theft victims reported experiencing negative feelings and emotions—including being worried or anxious (55%), violated (47%), vulnerable (42%), angry (36%), and mistrusting (29%)—while an equal percentage reported physical problems associated with their case, particularly trouble sleeping (37%), stress (35%), and persistent pains or headaches (24%). More than half also reported that identity theft contributed to problems with an employer (58%), family (76%), or friends (79%).[5]

A growing number of smaller-scale studies offer supporting evidence of each of these types of harms. First, studies consistently show that being a victim of

[3] Harrell, Erika. 2019. *Victims of Identity Theft, 2016*. Washington, DC: Bureau of Justice Statistics at 11. ("DOJ Report.")
[4] DOJ Report at 10.
[5] Identity Theft Resource Center, *2022 Consumer Impact Report*, at 27-34, https://www.idtheftcenter.org/post/identity-theft-resource-center-2022-consumer-impact-report-reveals-effects-social-media-account-takeover/ ("ITRC 2022 Report")

a data breach or identity theft can affect a consumer's physical and mental health. Such consumers often develop sleep problems, stress, back pain, headaches, high blood pressure, and other physical symptoms like loss of appetite.[6] Worse still, victims of medical identity theft (when personal information is used to fraudulently acquire medical care) may receive incorrect and potentially life-threatening medical diagnoses or treatment due to errors in their medical files.[7] Psychologically, data breaches and identity theft can leave consumers anxious or insecure about the future.[8] Victims report that they feel angry, violated, vulnerable, or depressed, while some even consider suicide.[9] Moreover, identity theft can precipitate mistrust in other people; organizations like businesses, financial institutions, and government agencies; and systems like financial markets.[10]

---

[6] *Id.*; *see also* Randa, Ryan, and Bradford W. Reyns. 2019. "The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey." *Deviant Behavior* 1–15. doi: 10.1080/01639625.2019.1612980.

[7] Andrews, Michelle. 2016. "The Rise of Medical Identity Theft." *Consumer Reports*, August 25; Dixon, Pam, and John Emerson. 2017. "The Geography of Medical Identity Theft." World Privacy Forum. www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf

[8] Brensinger, Jordan. N.d. "Identity theft, Mistrust, and the Production of Economic Insecurity." Unpublished manuscript (hereafter, Brensinger, "Economic Insecurity"); ITRC 2022 Report at 32; Identity Theft Resource Center. 2021. "2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends, and Workplaces." https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/, (" ITRC 2021 Report"); Kilovaty, Ido. 2021. "Psychological Data Breach Harms." *SSRN Electronic Journal*. doi: 10.2139/ssrn.3785734; Sharp, Tracy, Andrea Shreve-Neiger, William Fremouw, John Kane, and Shawn Hutton. 2004. "Exploring the Psychological and Somatic Impact of Identity Theft." *Journal of Forensic Sciences* 49(1):1–6; Solove, Daniel J., and Danielle Keats Citron. 2018. "Risk and Anxiety: A Theory of Data-Breach Harms." *Texas Law Review* 96(4):737–86.

[9] ITRC 2021 Report; ITRC 2022 Report; Sharp et al. "Exploring the Psychological"

[10] *Id.*

In terms of relational harms, some studies show that identity theft can generate interpersonal difficulties, such as an increase in conflict with and a perceived lack of support from one's family or friends.[11] In some types of identity theft, consumers have even faced having their children taken away by authorities responding to fraudulent data in their records.[12] Inadequate information security can therefore negatively impact consumers' relationships to those around them.

Lastly, identity theft can result in reputational injuries to consumers. As data is increasingly used for reputational purposes, including in hiring, housing, insurance, and even dating, errors can have far ranging consequences.[13] Damage to these forms of reputation lead some individuals to avoid pursuing resources and opportunities ranging from formal employment to volunteering in their children's schools.[14] Moreover, many consumers express awareness of the stigma associated with negative marks on their credit reports and criminal records and so feel shame at having such marks, even when they know they are not responsible.[15] Perceived

[11] ITRC 2022 Report at 27; ITRC 2021 Report at 19-20.
[12] Andrews, "The Rise of Medical Identity Theft"; Dixon and Emerson, "The Geography of Medical Identity Theft."
[13] *See, e.g.*, Eubanks, Virginia. 2017. *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press, p.1-13; James. 2015. "Guide to Criminal Identity Theft." Identity Theft Resource Center. https://www.idtheftcenter.org/guide-to-criminal-identity-theft/); Lageson, Sarah Esther. 2020. *Digital Punishment: Privacy, Stigma, and the Harms of Data-Driven Criminal Justice*. New York: Oxford University Press, p.113-35; Perl, Michael W. 2003. "It's Not Always about the Money: Why the State Identity Theft Laws Fail to Adequately Address Criminal Record Identity Theft Comment." *Journal of Criminal Law & Criminology* 94:169–208; Rona-Tas, Akos. 2017. "The Off-Label Use of Consumer Credit Ratings." *Historical Social Research* 42(1 (159)):52–76.
[14] Lageson, S. E. 2016. "Found Out and Opting Out: The Consequences of Online Criminal Records for Families." The ANNALS of the American Academy of Political and Social Science 665(1):127–41.
[15] Brensinger, Jordan. 2022. "Producing Consumer 'Identities': Identity Theft and Insecurity in the Data Economy." PhD Dissertation, Department of Sociology, Columbia University. p.127-9; ITRC 2022 Report; Lageson, *Digital Punishment*, p.126-35.

and actual reputational damage thereby fuels further psychological and social harms.

Recent work by Jordan Brensinger, one of the contributors to this comment, documents many of these impacts in considerable detail.[16] In particular, his research found that victims' race and class backgrounds shaped how identity theft impacted their sense of trust and financial security. Following identity theft, low-income individuals and people of color often felt suspicious of people around them–including family and friends–and reported cutting ties or avoiding offering or soliciting informal assistance like letting people stay in their home in order to protect themselves and their personal information. By contrast, middle- and upper-income and white people tended to blame organizations and demand their protection.

As Brensinger's research illustrates, many of the issues described above disproportionately harm low-income individuals and people of color. While some research suggests that middle- and upper-income individuals are at higher risk of identity theft in general,[17] low-income individuals may experience more severe cases with greater financial losses.[18] Many non-pecuniary harms appear to trace

[16] Brensinger, "Economic Insecurity"
[17] Anderson, Keith B. 2006. "Who Are the Victims of Identity Theft? The Effect of Demographics." Journal of Public Policy & Marketing 25(2):160–71; DOJ Report; Reyns, Bradford W., and Billy Henson. 2016. "The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory." International Journal of Offender Therapy and Comparative Criminology 60(10):1119–39.
[18] Copes, Heith, Kent R. Kerley, Rodney Huff, and John Kane. 2010. "Differentiating Identity Theft: An Exploratory Study of Victims Using a National Victimization Survey." Journal of Criminal Justice 38(5):1045–52; Reynolds, Dylan. 2020. "The Differential Effects of Identity Theft Victimization: How Demographics Predict Suffering out-of-Pocket Losses." Security Journal. doi: 10.1057/s41284-020-00258-y.

these disparities, with individuals from marginalized communities reporting more severe psychological and emotional symptoms.[19] Moreover, as mentioned above, low-income individuals and people of color appear more likely to localize suspicion to their personal network, with potentially harmful consequences to their relationships and communities.

Together, the considerable physical, mental, relational, and reputational harms—as well as their disparate impact on low-income individuals and people of color—support requiring stronger security measures to prevent the significant non-pecuniary harms experienced by consumers.

B. Data security rulemaking

Businesses and consumers benefit from clearer rules and guidance on how to protect consumer data. The fact that several states have begun to regulate in this area speaks to the importance of data security for consumer protection. (*See, e.g.*, New York's SHIELD Act of 2019, N.Y. Gen Bus. Law§ 899-bb.) The Commission can use its considerable experience developing effective rules for financial services firms in the FTC Safeguard Rule to develop similar rules for businesses that deal with other valuable consumer information.

In particular, many of the key elements of the FTC's Safeguards Rule are not expensive to implement and are typically available in the off-the-shelf security

---

[19]Randa, Ryan, and Bradford W. Reyns. 2019. "The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey." Deviant Behavior 1–15. doi: 10.1080/01639625.2019.1612980.

packages or from online service providers. Such measures start by having an information security program with administrative, technical, and physical safeguards designed to protect customer information. The elements of such a program include, among other things, conducting a risk assessment, implementing and reviewing access controls, encrypting customer information at rest and in transit, disposing customer information securely, logging authorized users' activity, and keeping the information security program current.[20] The specific details around the requirements can be tailored to the size and sophistication of the business, but all businesses would benefit from establishing clear security standards.

II. The Commission should promote public oversight of automated decision-making systems. Existing consent-based frameworks are not sufficient to counteract potential harms. (Questions 53-54; 65-66; and 73-80.)

The Commission is correct to highlight the challenge of how regulators should address the growing use of automated decision-making systems to mediate the interactions between consumers and businesses. Such systems, when appropriately designed, have the potential to benefit consumers. But when they are poorly designed, they can have widespread and pernicious effects, especially for vulnerable consumers.

[20] *See* FTC Safeguards Rule: What Your Business Needs to Know, May 2022, https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know.

In particular, because automated systems rely on statistical patterns to make determinations, errors in such systems are inevitable. Errors can enter the system through a few different points. *First*, input data reflecting existing societal biases can lead to unfair outcomes.[21] *Second*, sparse data about certain populations might result in poorer predictive performance.[22] *Third*, opaque models can mask unfair or biased decisions by drawing hidden correlations based on protected categories that are unlawful.[23] *Fourth*, models can make spurious correlations that lend credibility to predictions that are often no better than coin flips and would be rejected if made by a human decision maker.[24] *Fifth*, models can fail when they are used outside the context for which they were designed.[25]

Despite the consequential errors that may result from the use of such systems, consumers often have limited visibility into how these decisions about them are made. Companies often claim that the models they are using are "trade secrets,"[26] and do not disclose any details about the decision-making process to the consumers. As a result, when errors are made based on flawed or incorrect data,

[21] Gebru, Timnit; and Buolamwini, Joy. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". Conference on Fairness, Accountability, and Transparency. 2018.
[22] Larrazabal, Agostina J.; Nieto, Nicolás; and Victoria Peterson. "Gender imbalance in medical imaging datasets produces biased classifiers for computer-aided diagnosis". Proceedings of the National Academy of Sciences (PNAS). 2020.
[23] Angwin, Julia; Larson, Jeff; Mattu, Surya; and Kirchner, Lauren. "Machine Bias". ProPublica. 2016.
[24] Narayanan, Arvind. "How to recognize AI snake oil". 2019.
[25] *See e.g.,* Ben Burgess, Avi Ginsberg, Edward W. Felten, Shaanan Cohney. "Watching the watchers: bias and vulnerability in remote proctoring software". USENIX Security Symposium 2022. Discussing the repurposing of facial recognition models for anti-cheating software.
[26] Rudin, Cynthia; Wang, Caroline; and Coker, Beau. "The Age of Secrecy and Unfairness in Recidivism Prediction". Harvard Data Science Review. 2020.

consumers lack the information necessary to challenge and correct these decisions.

Moreover, even if an individual consumer is provided an explanation about the output of an automated decision making system, that information will often be insufficient to detect problematic patterns like discrimination. An individual denied an opportunity can be given a perfectly reasonable-looking explanation that is consistent with their data, but will not have the ability to detect whether opportunities are being systematically denied to them, e.g. more women are rejected than men.[27] In order to detect group-level disparities, some trusted entity would need more comprehensive monitoring or auditing abilities to evaluate the system as a whole to understand the decision choices.

A major obstacle to uncovering flaws in automated decision making systems is that researchers do not typically have access rights to test the models. When, for example, researchers gained access to a widely used healthcare model, they were able to identify systematic biases in the system and propose changes to mitigate those risks.[28] But such access is rare. For example, researchers who study the ad-delivery algorithms of major online platforms are stymied by the limited visibility the platforms afford them,[29] despite studies showing how these

[27] *See* Ayelet Gordon-Tapiero, Alexandra Wood, and Katrina Ligett. 2023 (forthcoming), "The Case for Establishing a Collective Perspective to Address the Harms of Platform Personalization," *JETLaw* 25, 4. Draft available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4105443
[28] Obermeyer, Ziad; Powers, Brian; Vogeli, Christine; and Mullainathan, Sendhil. "Dissecting racial bias in an algorithm used to manage the health of populations". Science. 2019.
[29] *See e.g.*, Megan Bobrowsky, *Facebook Disables Access for NYU Research Into Political-Ad Targeting,* Wall Street Journal, Aug. 4, 2021, https://www.wsj.com/articles/facebook-cuts-off-access-for-nyu-research-into-political-ad-targeting-11628052204 .

automated ad-delivery systems can perpetuate biases in ads concerning housing and employment.[30]

In other words, relying on making incremental improvements to the existing notice & consent framework to fix these algorithmic discrimination problems through, for example, better explanations is a mistake. Numerous studies have shown that the notice & choice framework is deeply flawed.[31] Most consumers simply do have the time or ability to digest the inner workings of complicated automated decision making systems to make informed choices. More importantly, many of these systems are deployed in environments where consumers lack the ability to choose meaningful alternatives. Instead, the Commission should consider requiring systems to have substantive protections for consumers that are built in by default. Consumers should have the right to review, challenge, and correct the data about them that is used to make automated decisions. They should also have access to details about the model that led to adverse actions. While such notices are mandated in financial decisions, they are not implemented in most other domains. And there should be a system for third party auditing of systems. Finally, the Commission should also consider requiring automated systems to provide functionality for consumers to exercise their choices through collective mechanisms or agents, and torespect the automated signals that users may send to such systems.

[30] *See* Imana, Basileal; Korolova, Aleksandra; and Heidemann, John. "Auditing for Discrimination in Algorithms Delivering Job Ads". Proceedings of The Web Conference (WWW). 2021.
[31] *See e.g.,* Joel R. Reidenberg et. al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & Pol'y for Info. Soc'y 485 (2015).

* * *

In closing, we appreciate the opportunity to provide these initial comments and look forward to further opportunities to engage with the rulemaking process.

Respectfully submitted,

Nia Brazzell
Emerging Scholar

Jordan Brensinger
Postdoctoral Research Associate

Shaanan Cohney
Lecturer, University of Melbourne

Sayash Kapoor
Graduate Student, Computer Science

Mihir Kshirsagar
Clinic Lead

Katrina Liggett
Microsoft Visiting Professor

Jonathan Mayer
Assistant Professor of Computer Science and Public Affairs

Arvind Narayanan
Professor of Computer Science

Contact: 609-258-5306; mihir@princeton.edu