The Slow Violence of Surveillance Capitalism

How Online Behavioral Advertising Harms People

Yuxi Wu
yuxiwu@gatech.edu
Georgia Institute of Technology
Atlanta, GA, USA

Sydney Bice
sbice7@gatech.edu
Georgia Institute of Technology
Atlanta, GA, USA

W. Keith Edwards
keith@cc.gatech.edu
Georgia Institute of Technology
Atlanta, GA, USA

Sauvik Das
sauvik@cmu.edu
Carnegie Mellon University
Pittsburgh, PA, USA

ABSTRACT

People's negative reactions to online behavioral advertising (OBA) are well-documented. However, past work has primarily focused on cataloguing these reactions and exploring how to change them, rather than understanding the ways these negative reactions affect people's lived experiences. Drawing upon scholarship on socio-technical *harms* in human-computer interaction and computer-supported cooperative work, we investigate and categorize the different ways people report having been harmed by OBA. Through an online survey with 420 participants, we identified four key harms arising from OBA: psychological distress, loss of autonomy, constriction of user behavior, and algorithmic marginalization and traumatization. We next discuss the "slow violence" inflicted by OBA and the normalization of people's affective discomfort with OBA, and how the two can present an opportunity for researchers to re-conceptualize OBA—and the invasive data practices it entails—as not just abstractly concerning to people, but as actively harmful.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; • **Human-centered computing → Empirical studies in HCI**.

ACM Reference Format:
Yuxi Wu, Sydney Bice, W. Keith Edwards, and Sauvik Das. 2023. The Slow Violence of Surveillance Capitalism: How Online Behavioral Advertising Harms People. In *2023 ACM Conference on Fairness, Accountability, and Transparency (FAccT '23), June 12–15, 2023, Chicago, IL, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3593013.3594119

1 INTRODUCTION

> *Surveillance capitalism unilaterally claims human experience as free raw material... It is obscene to suppose that this harm can be reduced to the obvious fact that users receive no fee for the raw material they supply...the essence of the exploitation here is the rendering of our lives as behavioral data for the sake of others' improved control of us.*
> — Shoshana Zuboff [49]

Surveillance capitalism—the profit-driven collection and commodification of personal data by private corporations—has resulted in the gradual erosion of privacy, leaving people with "no exit, no voice, and no loyalty; only helplessness, resignation, and psychic numbing" [49]. Its key driver: online behavioral advertising (OBA), or "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests." [18]

While OBA has been touted as a way to efficiently match advertisers and users, people have myriad concerns about the practice. They dislike not only the specificity of their targeting but also their abundance and ubiquity, not to mention generally finding them "creepy" [22, 27, 43, 48]. All-in-all, there has been extensive documentation of the negative ways that people respond to OBA. However, we know comparatively less about how OBA materially harms people, especially through its entanglement with modern daily life. As Zuboff describes, "there are consequences to this diminishment of rights that we can neither see nor foretell" [49].

The concept of *harm* is both a colloquial and legal one: according to Black's Law Dictionary [2], it is defined as "injury, loss, damage; material or tangible detriment". Defining privacy harms is of increasing interest in legal scholarship [12, 15]. Whereas financial losses and physical injury can be clearly identifiable as harms in a court of law [15], privacy harms like those entailed by OBA are less well-understood and often unrecognized. For example, a user might be alarmed to see embarrassing personal shopping history pop up in targeted ads on a work device. Or, they might feel spied on when they see a targeted ad for a product they thought they only discussed out loud with a friend. Insidiously, however, these small, seemingly mundane events can accumulate into a loss of control over interpersonal context and being constantly surveilled without consent [49]—in other words, a lived experience of fear and powerlessness [6].

Other experiences with OBA can be more evidently harmful. Advertisers, implicitly or explicitly, can infer and target specific sensitivities and vulnerabilities to increase clicks and sales: e.g., mental and physical health conditions [13]; demographic characteristics like age, gender identity, sexual orientation, race, etc.; bereavement; and unhealthy body stigma [20]. Ads based on these personal and psychological vulnerabilities can entail harmful consequences:

FAccT '23, June 12–15, 2023, Chicago, IL, USA

ACM ISBN 979-8-4007-0192-4/23/06.
https://doi.org/10.1145/3593013.3594119

users might, e.g., call their self image into question or reveal details about their personal identity without their consent.

In this work, we ask, "**How does online behavioral advertising harm people?**" Through a survey of 420 participants online, we investigated and categorized people's lived experiences of harm from OBA. Specifically, we asked participants to share with us a recent privacy-violating experience with OBA that they felt was personally impactful. In analyzing these accounts, we identified four main types of harms arising from OBA:

(1) *Psychological distress.* Broad negative mental or cognitive effects related to OBA.
(2) *Loss of autonomy.* Denial or limiting of opportunity to make own choices.
(3) *Constriction of user behavior.* Alteration of user interactions with technical systems in response to other OBA harms.
(4) *Algorithmic marginalization and traumatization.* Harms specific to personal characteristics (i.e., demographics) or vulnerabilities (e.g., sensitive medical information).

We then contextualize users' tendency to normalize these harms within both the concept of "slow violence" [20, 32], and a legal landscape that struggles to recognize privacy harms as concrete injuries [12, 15]. We argue that FAcct, HCI, and privacy researchers have an imperative to consider these contexts in future work, so as to help legitimize these experiences as harms to be mitigated and worth redress. In our analysis, we also suggest two potential first steps for future work: empirical measurement of the four types of OBA harms we identified, and documentation of protective actions that people have taken to evade these harms. In so doing, we can facilitate the formal recognition of OBA harms and institute processes to mitigate and redress these harms.

To summarize, we make two key contributions in this paper:

- A typology of privacy harms from OBA based on a large-scale empirical study.
- A discussion of how formal recognition of OBA's privacy harms can be a first step to alleviate them.

2 RELATED WORK

In this work, we examined how OBA can harm people. We build on prior work of not only user perceptions of online behavioral advertising—including attempts to change these perceptions, such as through user education and increased transparency—but also harm in socio-technical systems.

2.1 Online behavioral advertising

Online targeted ads are highly effective at engaging users to click. Broadly speaking, however, people have various reasons to dislike online targeted ads, finding them creepy, privacy-invasive, and disruptive [7, 22, 39, 42, 43, 47, 48]. We build on this by specifically examining negative *effects* of OBA on people's lived experiences, beyond descriptive perceptions of or affective responses to OBA. We view these effects through a lens of harm, which we ground in literature discussed in more detail in the following subsection. Past work on the harms of ad targeting has primarily focused on targeting based on political interests, which can limit user exposure to diverse viewpoints [9, 10] (a phenomenon reinforced and exacerbated by the ad delivery mechanisms themselves [4]). However, as Gak et al. [20] point out, what an ad algorithm deems as "interests" can easily be someone's vulnerability, e.g., sensitive health topics like weight-loss ads. In our work, however, we examine not just the harms of sensitive "interest"-based targeting, but also broad emotional and psychological harms to autonomy and the way people go about their day-to-day lives.

Mental models and folk theories also influence the way that people approach and respond to OBA. Yao et al. [47] found that user understanding of OBA can vary along three dimensions: who tracks the user's information, where the information is stored, and how the ads are delivered. To address these perceptions, prior work has tried to increase user awareness and agency about OBA, primarily via greater algorithmic transparency [27, 33, 44, 45] and providing more user controls to hold advertisers accountable; two thirds of the FAccT field name itself—Accountability and Transparency—mirror this tendency. But these approaches can also harm people. For one, online privacy notices can be confusing or too long for users to read [25, 28]; users who *do* read them can become alarmed and carry greater psychological burdens with the knowledge that their privacy is being violated [19, 27, 30]. More user control also does not mean more privacy [11], but can rather burden users further [40]. Finally, as we will show in the sections to come, when people believe they have exhausted all possible avenues to evade targeted ads, they feel frustrated and trapped.

Further, even with transparency and awareness measures in place, people might not take advantage of such measures or trust in advertisers and corporations to fully protect their privacy. As Lee et al. [27] found, users reject viewing explanations for targeted ads due to a sense of helplessness and resignation: since they felt powerless to change anything about the targeting, they did not want to know more about it. As another example, news media has frequently debunked the myth that Facebook secretly listens to real-life conversations via users' mobile phones and targets ads from those conversations; however, people persistently believe this rumor due to mistrust in Facebook and Meta. Das et al. help explain why through a recent review of barriers to end-user privacy and security behaviors [16]: awareness is only one barrier that must be overcome—people also have low motivation because they feel helpless, and have little ability to verify and control what data harvesters collect. In our work, we also explore the ways that this mistrust and helplessness burdens and harms people.

2.2 Harms and socio-technical systems

We draw upon a rich history of literature in the fields of computer-supported cooperative work (CSCW), human-computer interaction (HCI), and FAccT that examines the relationship between computing and social justice, and how users can be oppressed and marginalized by such systems [5, 8, 13, 14, 31]. For example, Seberger et al. [37] distinguish between the "power to" do something technical that a particular app grants a user, and the "power over" the user that the app and its institutional back-end has over the user; this tension forms a user ambivalence to privacy that opens the door to more invasive data practices. Related work [38] found that this "affective discomfort" has become normalized in the user experience. In our work, we explore how OBA can inflict this persistent feeling and how it harms users.

OBA also leads to specific harms of its own. As discussed previously, people exhibit negative affective responses to OBA, disliking their repetitive nature [48] and the specificity of their targeting [43]. Milano et al. [29] also proposed a taxonomy of *potential* harms primarily based on the content and context of OBA: (1) bad content (e.g., using sexist stereotypes to promote a shaving product to men), (2) omission of essential content (e.g., hard-to-reach communities not seeing public health ads for a vaccine), (3) exploitative context (e.g., exploiting users' personal vulnerabilities, similar to [20]), and (4) deprived context (e.g, a job-seeker not seeing job ads in their area). And, more recently, Gak et al. [20] previously extensively examined the specific relationships between targeted weight loss ads and users with histories of disordered eating, and the consequent harms of that relationship.

Prior work has not, to our knowledge, analyzed *user-reported* harms of OBA *generally*. We hope to show in our work that OBA, coupled with its inextricability from modern daily life, causes evident harms in people's day-to-day lives. We situate our contributions in the broader landscape of *privacy harms*, theorized by both Calo [12] and Citron and Solove [15], who assert that harms from privacy violations are currently inconsistently recognized by courts, and that certain non-financial and non-physical harms from privacy violations should be as cognizable as financial and physical ones. As we will argue in Section 5, the FAccT, HCI, and privacy communities have a similar imperative to legitimize these harms and recognize user experiences as human experiences.

	Shared experience	Did not share
Age		
18-24	86	31
25-34	111	26
35-44	47	19
45-54	28	10
55-64	27	13
65+	11	6
Gender Identity		
Female	174	57
Male	119	42
Genderqueer/Non-conforming	7	3
Trans Male/Trans Man	8	1
Different Identity	3	0
Ethnicity		
White	245	85
Black	17	6
Asian	22	4
Mixed	18	9
Other	13	1
Education		
Less than high school	12	1
High school diploma	69	25
Technical/community college	50	11
Undergraduate degree	127	44
Graduate degree	46	17
Doctorate degree	7	5
Total	**315**	**105**

Table 1: Demographics of participants, broken down by whether they chose to share an account of their experiences with online behavioral advertising (OBA).

3 METHODOLOGY

While the literature is clear that people find OBA creepy, unsettling, and threatening, how OBA materially and negatively impacts lived experience remains unclear. Building on prior work systematizing the harms of socio-technical systems, we aimed to systematize the many concrete ways OBA can harm. We conducted an online survey on Prolific, a crowd-work platform, with 420 participants who had indicated in a screener questionnaire that they had previously experienced a privacy violation related to online targeted or behavioral advertising.

3.1 Recruitment, ethics, compensation

We first screened 1275 potential participants by asking them if they had recently experienced feeling violated by OBA. These potential participants were adults located in the United States, fluent in English, and active users of Internet-based services like social media, a smartphone, or a smart home device. This screener took on average less than a minute to complete; participants were compensated 0.25 USD on the Prolific platform. Those who answered "yes" to the screener (n=420) were recruited to participate in the main study, a short survey hosted on Qualtrics. The main survey took on average 5 minutes, for which participants were compensated 1.50 USD. Our study was approved by the Georgia Tech IRB.

3.2 Survey

There were three main components to the survey. First, after reminding participants that they had previously told us that they had a recent privacy-violating experience involving OBA, we asked if they wanted to tell us about the experience in more detail. Because such experiences can be sensitive in nature and difficult to talk about, we gave participants the option not to tell us about the experience at all. Second, if a participant agreed to share their experience, to encourage richer qualitative contributions beyond simply describing it as "creepy", we suggested details to include in their account of the experience: the parties and information involved, any actions they took in response to the incident, emotional reactions, changes in how they used the Internet, or why the incident was personally impactful. If a participant chose not to share an account, to ensure participants were being equally compensated for the same amount of work, we asked them if there were other privacy harms or violations unrelated to OBA they would be willing to share instead. Finally, we asked the participants why they did or did not, respectively, choose to contribute to our study.

3.3 Analysis

To understand the many ways OBA can harm or burden people, we applied an inductive approach to qualitative data analysis. One member of the research team read through each of the accounts provided by participants and performed open coding, iteratively updating the codebook as necessary. The researcher then performed an initial round of axial coding to consolidate codes into different types of reactions to online targeted advertising, as well as any descriptions of the content of the ads or where the experience took place. A second researcher independently coded the data according to the codebook. Through multiple discussions, all members of the research team consolidated and synthesized the concepts into broader categories. The codebook, grouped by preliminary categories, can be viewed in Appendix A.

The qualitative accounts, by their privacy-violating nature, described how online targeted ads negatively affected participants. We thus grouped codes and concepts based on the nature of the negative effect the experience had on the participants; more specifically, we examined them through a lens of harm. As aforementioned, through our coding process and multiple iterative discussions, and taking inspiration from prior work [15, 20, 48], we developed four broad categories of harms that we summarize in Table 2 and discuss in detail in Section 4.

4 FINDINGS

We first provide a demographic breakdown of participants based on whether they chose to contribute an account of their experiences. We then report on a broad overview of the online platforms where these accounts took place. Finally, in the bulk of the section, we discuss four broad categories of harms that can arise from online behavioral advertising: psychological distress, loss of autonomy, behavior constriction, and algorithmic marginalization and traumatization. We note that these harms are not mutually exclusive, but have distinguishing characteristics as described in Table 2.

4.1 Quantitative breakdown

4.1.1 Participant demographics. In total, 315 participants chose to share an account; 105 chose not to. A summary of the demographics of our participants can be found in Table 1. They are grouped by whether or not they chose to contribute an account of their experiences.

4.1.2 Where accounts took place. Over half of participants mentioned specific companies or websites as the source of their experiences with OBA. Meta products were the most-mentioned site of violating experiences, with 84 participants mentioning an experience involving Facebook, and 55 mentioning Instagram. 49 participants mentioned Google, and 18 mentioned YouTube specifically. 20 participants mentioned Amazon or Alexa devices. Only 5 participants mentioned TikTok. 140 participants did not name any specific company or site; however, 34 of these participants mentioned seeing ads on "social media" generally, and 10 participants said the advertising was "everywhere".

4.2 Psychological distress

Psychological harms involve a wide range of negative mental responses, but typically fall into two primary buckets: emotional distress, i.e., painful or unpleasant feelings; and disturbance, i.e., disruption to peace of mind. In the following subsections, we discuss different examples of both types of psychological harms.

4.2.1 General emotional distress. As Citron and Solove argue [15], one of the most common types of harm caused by privacy violations is emotional distress. Our participants' experiences provide empirical support for this claim: a fifth of accounts mentioned feeling unsettled by or uncomfortable with the specificity of targeted ads. For example, P326 expressed discomfort with the uncertainty and lack of transparency on what data is collected and the inferences that could be made thereof: *"[Google] knew I was interested [in a new phone] because I had said so, out loud, to my girlfriend on a private call. If they hear that, who knows what else they hear? And what could be done with that information?"*

4.2.2 Disruption of browsing experience. Other participants expressed that the targeted ads disrupted their normal browsing experience. For example, P284 was angry and frustrated with seeing ads after they finished comparing an item's price at Walmart: *"I was done needing to see Walmart, and now it's all over the searches and websites afterward."* Similarly, other participants felt that they wanted to search for things independently, rather than have that search be re-incorporated into an ad targeting experience: *"You can't just search anything anymore without being bombarded by ads"* (P171). Some participants saw so many targeted ads that they had trouble distinguishing what was an ad: *"I lose track of the number of real posts I see [on Facebook] vs. ads these days"* (P160).

4.2.3 Information redundancy. Sometimes, the sheer amount of targeted advertising from *specific* advertisers resulted in participants being oversaturated with redundant information. For example, P188 was frustrated with repeatedly seeing the exact same ad from Halara, a clothing retailer: *"After the third time I felt very frustrated and bored. This ad was haunting me and honestly I don't think I would buy from this company now. It annoyed me so much. I would mute my computer while it played and try to skip it as soon as possible."* Another participant who was targeted with ads from a guitar retailer said they were *"inundated with advertising...for other guitars on unrelated sites repeatedly. This presumes upon my attention and cognitive/emotional space and angers me"* (P243). This inundation could also translate to a loss of time and effort in real life. P154 noted that even if they had blocked ads *online*, they still received corresponding physical marketing in the mail: *"I've cleared my cache and cookies since but I'll be receiving snail mail for generations. I get angry about this marketing because it consumes my time to throw everything away...I have to shred every offer that comes in the mail. Waste of paper, waste of resources, waste of time and energy."*

4.2.4 Questioning own browsing behavior. Beyond feeling annoyed or overwhelmed by targeted ads, however, we also found that participants frequently tried to guess at where the ads came from. This echos prior work [27] that found that users wanted explanations for ad targeting explanations to confirm their own preconceptions of how their data was collected or the motives of advertisers. For example, multiple participants mentioned that ads "must have" come from their browsing and search history or their online chats with friends and family. P358 surmised that ads related to their personal shopping showed up on their work computer due to sometimes logging into their personal accounts at work: *"We are a Microsoft-based system [at work] but at times I have clients send me Google Drives, etc. which requires me to log into my Gmail. I suspect that is how these ads came to be on my work computer."* Some participants approached ads like a mystery to be solved with breadcrumbs of all the places where they had encountered certain ads:

> *When I turned on another computer that I watch streaming television on, the same topic ads were on there, as well. I concluded that Google targets ads by your router's IP...and then dispenses ads to all machines connected that IP, through your router. If you look up porn, be aware that porn ads could show up on their computer,*

Harm	General description	Distinguishing characteristics
Psychological distress	Broad negative mental or cognitive effects related to OBA in general.	General emotional distress, i.e., painful or unpleasant feelings, or disruptions to peace of mind.
Loss of autonomy	Denial or limiting of opportunity to make own choices.	Lack of control or consent over not only targeting, but also secondary contexts like interpersonal relationships and purchasing behaviors.
Constriction of user behavior	Alteration of user interactions with technical systems in response to other OBA harms.	Losses in usability and utility of devices and services due to adopting additional privacy and security behaviors, as well as the time and resources associated with such evasive actions.
Algorithmic marginalization and traumatization	Harms specific to personal characteristics (i.e., demographics) or vulnerabilities (e.g., sensitive medical information).	Feelings of diminishment associated with highlighting user-specific characteristics, rather than broader senses unease or overwhelming.

Table 2: Descriptions of the types of harms and their distinguishing characteristics.

because of the general use of ads pointed at your domain. (P378)

Others expressed disgust at the tracking after after detailing their browsing behavior step by step. P248, for example, shared how they looked up a clothing brand in Chrome on a work device, and then saw related ads on their personal device while using Firefox: *"I clicked on those items in a different browser in a different physical location. I felt absolutely stalked by this ad."* Similarly, after retracing their digital breadcrumbs, some participants then expressed regret about mistakes they had made along the way when researching and discussing the related ad topics. P154 shared that they forgot to block cookies on a credit card website one time, and have regretted it ever since: *"I forgot to deselect the marketing cookies once on a credit card website...but now every single website has credit card offers."*

4.2.5 Paranoia from suspicion of eavesdropping. When their investigations into the origins of targeted ads reached dead ends, participants often felt that the only possible explanation was that their devices were eavesdropping on them. Several participants felt that merely mentioning a product in a real life conversation with a friend or family member would result in seeing ads for that product, whether it be spices (P42), cat food (P49), electric toothbrushes (P56), hula hoops (P90), or press-on nails (P131). While the concept of smart and mobile devices—in particular, Facebook and Meta—eavesdropping on users via microphones has been frequently debunked in popular news media and prior work [34], the myth persists. The lack of transparency and trustworthiness surrounding these ad targeting practices[6] necessitates misguided guesswork on the part of the users, which results in concrete harms: constant suspicion, fear, and paranoia.

The immediacy and consistency with which targeted ads appear made participants suspicious of their microphone-enabled devices: *"An Alexa device was in the same room, but was off, or so we thought. On more than one occasion the items we discussed showed up almost immediately on our devices (email, internet ads, social media, etc.)"* (P20). Similarly, P60 shares:

> *I don't have an Alexa or anything like that, but somehow my phone is apparently listening anyway? I don't know what to think. These are private conversations! And I know that I haven't just entered any of that into the search window on my phone or computer. It has happened far too many times for it to be coincidence and all I can assume is nothing is private anymore. It's sickening.*

Some more tech-savvy participants admitted that even though they were educated otherwise about microphone eavesdropping, they still felt concerned. For example, as P1 described, *"While I know rationally that these programs aren't listening, it is very unsettling that they are reading my data to target ads to me."* Similarly, P36 said they closed the Instagram app on their phone as soon as they were done using it, even though *"I know it supposedly doesn't listen in but rather tracks you in other ways...but sometimes the ads are a little too targeted for comfort"*. P55 adds that the targeting is simply too accurate and immediate to ignore: *"While it is possible that it's a coincidence and social media shouldn't have access to my microphone to capture data and tailor advertisements to me, I can't help but feel creeped out and paranoid that I'm being recorded at all times."* These persistent fears are direct vectors to psychological harm.

4.3 Loss of autonomy

Autonomy harms involve accounts where participants were prevented from making their own choices, either via being directly denied these choices, being tricked into thinking their choices were freely made when they were not, or being limited in the choices they could make. These harms recall Zuboff [50], who wrote that in surveillance capitalism, "the surest way [for advertisers] to predict behavior is to intervene at its source and shape it". In the following subsections, we discuss different types of autonomy harms.

4.3.1 Lack of consent or control over targeting. One of the most common concerns that participants voiced was that they did not consent to being targeted for online advertising. Some participants, for example, felt violated when they saw online advertisements based on purchases they'd made in a physical store. P77 shared how they had seen ads related to groceries they bought in a physical store, but had never expressly consented to connecting these purchases with any shopping website or app: *"I feel it should be against the law to...invade my privacy without express permission each time they want to do something like this."*

Others felt like they had no control over the nature of the targeting, even when the targeting was incorrect. For example, one participant was researching flooring materials on behalf of their mother, but still received endless ads related to it. They felt frustrated at being misunderstood:

> *The flooring isn't really for me, but just in my searching, I've had countless ads and emails sent to me about all kinds of flooring. I've even had other companies sending me info about flooring. I feel like I'm being attacked by salesman at a used car dealership and I really have no control over it.* (P351)

Other participants noted that even though they understood their data was being collected online, it still felt like a breach of consent. Participants found the pervasiveness and specificity of the ads overwhelming, describing a mission or scope creep of sorts: *"It's not even what I'm doing anymore, it's everything I am thinking"* (P49).

4.3.2 Lack of control over self-presentation. Several participants mentioned seeing ads on devices they used at work that were related to interests in their personal life, or vice versa. This exemplifies context collapse, or "how people, information, and norms from one context seep into the bounds of another" [17]. Participants who experienced context collapse felt they had little control over the consequences, usually in the form of the targeted ads unwittingly revealing private information about themselves.

One immediate harm of this phenomenon was social embarrassment, as P358 writes:

> *About a year ago, I had been shopping for lingerie for my honeymoon. This was only on my personal laptop. I had a coworker in my office looking up some information with me. I believe it was thesaurus.com or something like that, but I can't fully remember because what was ON the page was so mortifying. There, in front of my coworker, on my WORK computer, were specialized ads for lingerie. I was so embarrassed. I tried to ignore the ads that seemed to be disproportionately large on the screen. My coworker thankfully did not mention them, but now probably thinks I shop for lingerie while at work.*

Other participants noted that even friends who talk to them about sensitive problems could influence the ads they saw and result in negative outcomes. For example, P124 mentioned speaking to a friend about the friend's pending divorce, and subsequently got ads related to divorce lawyers. This made the participant concerned that their own spouse would accidentally see these ads and misinterpret them: *"This could potentially lead to misunderstandings with my spouse. What if I was showing them something on my phone and a divorce attorney ad came up?"*

Relatedly, participants also experienced context collapse with family members directly. P363, who had shared their Facebook credentials with their mother, described how their mother saw ads from their feed for explicit content and surmised that those ads were based on P363's own browsing behavior. The ads thus revealed private information about P363 to their mother without their consent, making P363's relationship with their mother *"uncomfortable for a long time"*. Another participant shared that a surprise birthday gift for their husband was ruined when the husband was targeted with ads related to the participant's search history. As a result of this ruined surprise (a harm in itself), they began altering the way they used the Internet out of persistent concern that future surprises could be ruined too:

> *I have started only using my desktop at work to search for presents for people in my family. I'm paranoid even to buy gifts for my parents and in-laws on our family computer, though they don't live with us and the chances they will use our family desktop to search the web is very small. But just in case one day they need to use the computer, I don't want them to see the gift I am searching for them!* (P192)

Similarly, P265, who researched medical treatments on behalf of a friend, felt constantly reminded of their friend's heart problems. They also now felt burdened with protecting not only their own privacy, but that of their friend, too: *"I was not looking up the information for myself, but for a friend. I cannot go to most sites without seeing ads for TAVR (transcatheter aortic valve replacement) and now other heart problems. I will be careful about searching for sensitive information for both myself and my friends"*. P239 offered a similarly sensitive account of searching for resources for their sister-in-law who was dealing with marital rape: *"I started seeing ads related to mental health to help rape victims. I do not know who actually made the ads. It was a constant reminder of the abuse that she went through."*

4.3.3 Encouraging negative purchasing habits. A few participants felt compelled to buy things they did not need because they kept seeing ads for them. For example, P35 described themselves as *"impulsive with my money"*, and said that a stream of targeted ads *"makes it hard to use social media when I see ads for clothing that I want but cannot afford."*

4.3.4 Limiting consumer choice. On the other hand, for some participants, companies that used OBA were so off-putting that it compelled them to limit their choice set of things to buy and shop elsewhere, so as not to reward bad behavior. Several participants stated that the fact the advertiser was directly pandering to them made them not want to purchase anything from that advertiser. For example, a few participants felt that if an advertiser was spending so many resources on marketing targeted toward them, it must be a signal of a deficiency in the products being advertised. P18 wondered, *"If they [an e-bike company] have the budget to spend so much on targeted advertising, what is wrong with their e-bikes? I wonder if they are charging too much or that the product is of much lower quality than their competitors."* More bluntly, P408 said, *"I become so disinterested and put off by these practices I look at other brands, and I would NEVER click on such an ad regardless of my level of seriousness to purchase such a product."*

4.4 Constriction of user behavior

As we argued previously, users can face usability burdens when dealing with online targeted ads. Multiple participants mentioned taking privacy-protecting measures, such as disabling advertising-related tracking, deleting accounts on retail websites, and erasing browsing history. But even though they went through so much effort, participants felt they could not escape the ads. Despite having all *"privacy flags available set to the maximum"*, P167 said, *"the tracking persists. I feel powerless to prevent this from occurring."* Not

only are the effort and time taken to implement these seemingly futile measures an unwelcome burden for the average user to bear, but users are also penalized with a loss in usability and utility when they are forced to use services or devices in less-than-optimal ways.

Perceptions of microphone eavesdropping elicited specific actions from participants. One participant mentioned disabling Siri on their iPhone *"so that it was not able to listen at all hours"* (P19), limiting themselves from accessing the full functionality or convenience of their personal phone. We acknowledge that disabling Siri was an active choice on the part of the participant, and the immediate inconvenience of not being able to use Siri might seem like an innocuous harm. However, it's easy to imagine a scenario where opting out of one tool can lead to more extreme consequences, or the cost of opting out is greater than simply switching off a button.

As one example of the former, P119 shared that after making therapy appointments online, they saw ads related to depression and PTSD. As a result, they stopped booking their appointments online and instead could only do so over the phone. While this might only appear to be a minor inconvenience on the surface, people with social anxiety or social phobia could find the idea of making a phone call paralyzing, and may rely on online booking services. (In Section 4.5, we discuss in detail harms that specifically come from ads with sensitive content or offensive profiling). And, as an example of the latter, P340 said that they had *"removed all [Amazon] Alexa devices from their home and shut down all web camera (sic)"*, entailing a not-insignficant amount of time unplugging and covering up all their devices, and not to mention the money lost on purchasing the devices in the first place.

Several other participants mentioned avoiding having conversations about potential purchases or changing the way they talk to their friends to steer clear of getting related ads. For example, as P259 put it, *"I take the approach 'the walls have ears' and typically act as if someone (like my boss, for example) were listening [in] on my conversation, because it's clear that what I say in private might not actually be private anymore."* P55 said, out of fear of eavesdropping, they started physically separating themselves from their phone: *"I don't carry my phone with me into other rooms if I am hanging out with someone and if I need to search something up, I have to go and grab my phone from wherever I left it. I feel the need to keep distant in order to maintain some sort of privacy and to ease my paranoia."*

4.5 Algorithmic marginalization and traumatization

OBA based on user interests can over-simplify those interests and hone in on user vulnerabilities. Echoing prior work [20], we found that when users identified as part of a sensitive "interest" group, they were particularly vocal about being violated. We distinguish these harms from general psychological distress (Section 4.2) due to how these ads diminish people by highlighting their specific personal characteristics or vulnerabilities.

4.5.1 Violation of boundaries. Some participants felt that certain information should simply be off-limits as a basis for targeting. For example, one participant dealing with the death of a loved one felt that targeted ads related to funeral services tried to exploit their private grief: *"It was inappropriate to intrude on our grieving with an attempt to get us to spend money on elaborate funeral services or gouging us for insurance"* (P130).

These limits also applied to medical histories. For one, even if participants felt that the medical treatments promoted in certain targeted ads were valid, they were still disturbed that data brokers knew about their medical history and targeted them for it. For example, P244 felt that they were shown ads related to substance abuse treatment programs because of their history of opiate abuse, and were upset with how Facebook concluded this about them: *"It reminded me of a very dark time that I would like to forget. I am not against the company or the treatment program, just how Facebook selected me for targeted advertising."* P273 felt that seeing ads related to a medical condition on Twitter, Instagram, and Facebook, *"was akin to a HIPAA violation."*

4.5.2 Amplification of self-consciousness. Multiple participants reported feeling discriminated against when they saw certain targeted ads. Some older female participants reported seeing ads related to menopause, and said they felt uncomfortable that so much attention was being drawn to their age. As P249 writes, *"Few women like to have this stage of life rubbed in their faces by a social network, for goodness' sake...I didn't feel ashamed; I felt really depressed. I don't like to dwell on things that basically say to me, 'Say, I hear you're growing OLD, girl!'"* P366, who self-identified as a woman, said they started seeing ads for Botox and plastic surgeons *"EVERYWHERE"* when they entered their age into Instagram; they felt this promoted ageism. To avoid these ads, P366 created a new account with a fake age (evoking Section 4.4).

Participants also felt misrepresented and hurt by ads referencing neurodiversity. P2 shared an experience with ads related to autism, which unsettled them not only due to the sensitive topic, but also misleading portrayals of autism:

> *I was recently diagnosed with autism. In the following week, I was getting tons of ads on Facebook about "holistic medications" and "lifestyle changes" that help people to be "less autistic." Additionally, I was getting sponsored content from Autism Speaks and moms in the community. The ads were hurtful. Autism is a neurotype, not something that can be "cured", especially by unregulated supplements or diets. I think targeted misinformation like this is extremely sinister.*

Similarly, specific representations of neurodiversity in targeted ads made participants self-conscious about how they were perceived by others in real life, and caused them to alter their browsing behavior. One participant felt hurt due to an ad that portrayed people with ADHD as *"closed off and goofy"*, and said that it *"showed [ADHD] to be more lighthearted than it actually was. Now I'm a bit more self-conscious thinking others have seen the advertisement and are judging me. Now I know to be more careful with what I search"* (P126).

4.5.3 Traumatic triggers. Ads related to eating disorders and body image can serve as constant painful triggers for participants, echoing prior work [20]. For example, P78, who actively participates on an anonymous eating disorder forum, started getting ads for both erectile dysfunction and weight loss programs. They felt that seeing these ads outside of the forum was *"damaging to my mental*

and ultimately physical health, as they are constant reminders of my restrictive eating problem." Similarly, P206, who discussed body image and weight issues with friends and family members, noticed *"an increase in various weight loss ads across my social media platforms. Instagram has given me ad after ad for diet plans and paid exercise programs. I felt like every ad I saw was pointing out my insecurities and confirming my embarrassment in my appearance. Since this started, I have felt very unsafe on the internet."*

In a similar vein, participants dealing with bereavement also felt that seeing ads related to funeral services prevented them from moving on with their grief. P341, completely exasperated, expressed regret at looking up headstones for their grandmother on Google: *"Well that was a mistake, because to this day I get reminded multiple times a day that I had to lay my grandmother to rest. I see multiple ads a day on Google, Facebook. I'm over it. I just want to be able to mourn and let it go. At this point I don't want to ever Google anything again."*

4.5.4 Fear of social exposure. Beyond the immediately obvious harms of reductive ads based on demographics, participants also worried about secondary social ramifications of such ads. For example, participants who were members of the LGBTQ community felt alarmed that data brokers had algorithmically profiled their gender identity and sexual orientation. For one, they expressed anxiety about how these characteristics were inferred in the first place, especially if they themselves had not yet come out. For example, P173 wrote:

> *I am closeted on Facebook (not out as trans, neutral name, lots of family members added, had not yet changed my pronouns on the site) and it started advertising products aimed specifically at trans men to me—[chest] binders, online medical services for HRT [hormone replacement therapy], etc. I had not shopped for any relevant products. I do not know why Facebook decided I was/am a trans man. I am anonymous on other Facebook products like Instagram, no mention of gender or pronouns there at all, let alone my correct pronouns.*

As another, more immediate danger, P164 shared how they were afraid of exposure of their gender identity at work. This fear also constricted how they used their phone at work:

> *My coworkers do not know that I am transgender. Before a meeting we were all...scrolling through our phones. I got a targeted ad for a trans pride flag that was large and very visible. I immediately got scared that people behind or beside me would see so I quickly closed my phone and put it away. Now I don't open my phone when I'm in the same room with coworkers. I'm not trying to get outed in an unsafe way.*

Participants who were already out were still concerned. P214, for example, described a conversation with their boyfriend about underwear unrelated to their sexual orientation, but seemingly led to targeted ads about underwear for gay men: *"It felt wrong, especially when being gay is criminalized in some countries and even demonized among communities in the U.S. It's potentially dangerous if someone else sees an ad that's targeted towards something private about you."*

5 DISCUSSION

Our participants shared personal accounts of how online behavioral advertising harmed them by disrupting their peace of mind, eroding their autonomy, impeding on their day-to-day lives, and predating on their personal vulnerabilities. Yet, many still prefaced their responses with qualifiers like, "it may not seem like a hugely violating deal" (P12). As Seberger et al. [38] write, these violations do not become "less catastrophic or problematic upon regular repetition" but rather normalized; the authors reference the salience of the word "creepy" in the consumer vocabulary as a proxy for the undefined, constant institutional rebalancing of user convenience against violating data practices.

The mundanity of targeted ads makes it difficult for users to devote specific attention to fighting it; as Gak et al. [20] argue, the embeddedness of harmful targeted ads in a typical user's digital experience typecasts them as "non-events" to which users become habituated and numb. Literary scholar Rob Nixon [32] coined the term "slow violence" to describe things like the normalization of seemingly small harms. Slow violence, as Nixon defines it, consists of "calamities that are slow and long lasting, calamities that patiently dispense their devastation while remaining outside our flickering attention spans". Originally conceptualized by Nixon in reference to environmental degradation and climate change, slow violence was adapted by Gak et al. [20] to OBA. In this section, we examine how giving legal recognition to this slow violence can be a first step to mitigating privacy harms on a systemic level. We then explore how we as researchers can better support users in achieving this recognition.

5.1 Legally recognizing privacy harms

As a start, as early as 1980, the Federal Trade Commission (FTC) has recognized that small harms, in aggregate, can be sufficiently substantial if suffered by a large number of people[1]. However, as regulators can only address a small fraction of these privacy harms at any given time, more attention is given to flashier violations that are well-understood to cause harm to users, e.g., large-scale data breaches like the Equifax breach in 2017, which resulted in hefty FTC fines. But these one-off, ad-hoc solutions don't necessarily mesh with the slow violence of OBA. For example, Wu et al. [46] found that when a group of users collectively preferred an apology from Instagram as a solution to offensive algorithmic profiling—in other words, a recognition of harm—security and privacy experts dismissed the users' preferences as naive and fraught with implementation challenges. In this way, as Nixon [32] argues, the extended temporality of slow violence hides a more sinister foundation of social inequality: the people who experience the small harms of OBA and surveillance capitalism have unequal education, access, and power relative to the security and privacy experts who dismiss them.

One remedial measure is recognizing privacy harms, legally, in the same light as other sorts of harm. Currently, courts do not recognize privacy harms that don't involve tangible financial or physical injury. However, as Citron and Solove [15] write, "Individuals whose privacy has been violated need to hear the message

[1]FTC Policy Statement on Unfairness. December 17, 1980. https://www.ftc.gov/legal-library/browse/ftc-policy-statement-unfairness

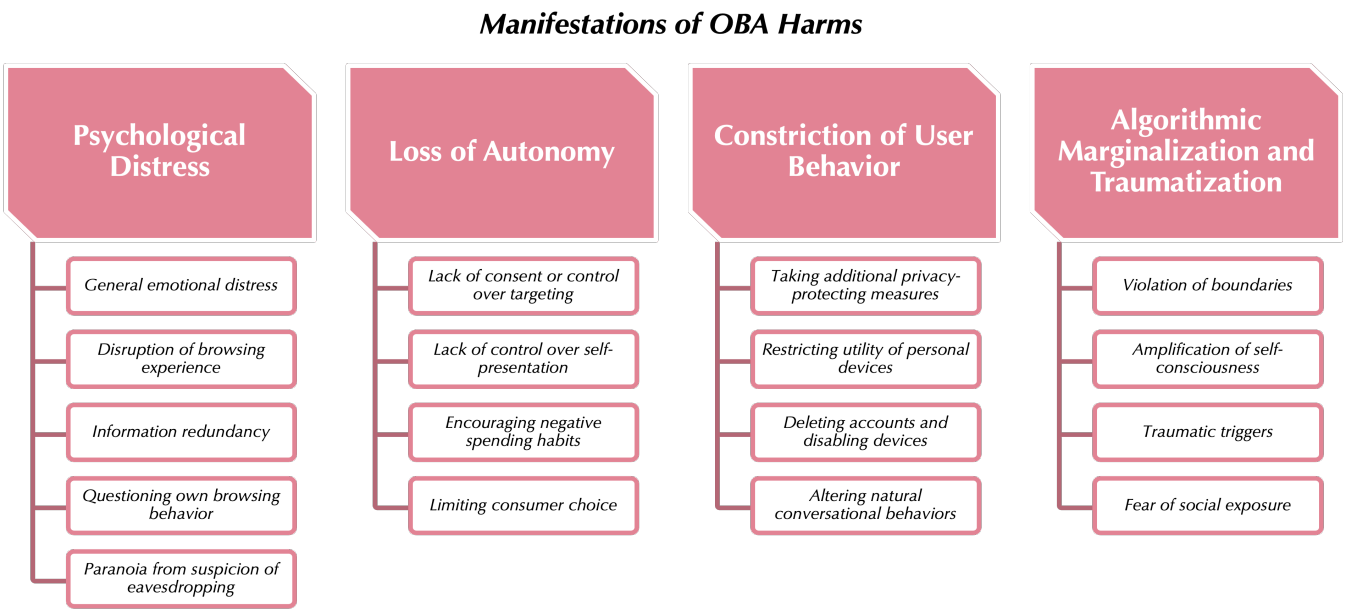

Figure 1: A summary of the ways we found OBA harms manifesting in people's lives. Aggregated, collective evidence of such experiences may help establish such harms as concrete injuries with legal standing.

that law is concerned with the harms they have suffered. Law's recognition of privacy harms tells individuals that their suffering is real and that their suffering is not just a fact of life that should be endured, but harm that should not be tolerated. Individuals can see themselves as harmed."

As one example, the targeted ads that could ostensibly result from microphone eavesdropping are, to users, indistinguishable from those based on cross-site tracking and algorithmic profiling. Both conceptualizations of OBA, regardless of actual practice, can lead to the same harmful outcomes of fear, distress, and unease in users, causing them to alter the way they handle their devices and hold conversations in real life. Thus, would more user education and transparency about the latter method being close to the truth than the former do anything to mitigate these feelings? Instead, a formal recognition that these harms carry a real burden can be used to actually redress those harms by, e.g., establishing legal precedent and allowing for the allocation of remedial resources (e.g., funding, headcount) to mitigate those harms.

5.2 Moving away from designing for the OBA "user experience"

Beyond legal recognition, we as FAccT, HCI, and privacy researchers also have an imperative to consider and mitigate harms. Developing tools and interfaces to increase user control and better educate users on how their data is being used is necessary but not sufficient to combat the slow violence of harmful targeted ads. As Seberger et al. [38] argue, these "solutions" may simplify privacy problems into bite-size, solvable pieces, but they fail to address the larger problem of the normalization of affective discomfort, which "perpetuates the associated conditions of exploitation and legitimizes invasive data practices that are detrimental to the diginity of *people*". Echoing prior arguments by Herley [23, 24] on why users choose not to take certain security advice, we contend the same for privacy: privacy dashboards, private browsing, and cookie blocking will not fully assuage people's privacy concerns. As we noted previously, regardless of what users did to enhance their privacy and security, the harms of the ads were already inescapable.

Instead of designing for discrete interactions between people and specific apps, we contend that the HCI privacy community should recognize these interactions and harms as being inextricable from larger societal concerns. As P167 suggests, our participants certainly already have:

> *My concerns with targeted and behavioral advertising aren't so much with any specific event but with the concept as a whole. The internet has become such a fundamental aspect of modern life that I can't just remove myself from the equation without significant impact.*

On these bases, we envision two intertwined areas of future work: concrete measurement of privacy harms, and documentation of the actions that users have taken to avoid harm.

5.2.1 Measurement of harm. As we've iterated throughout this paper, courts have expressed doubt that there is enough evidence to demonstrate a concrete harm from privacy violations (e.g., TransUnion LLC v. Ramirez [3, 41], and Spokeo Inc. v. Robins [1]). Yet, in our work, we have collected hundreds of accounts of the concrete ways that people are harmed by OBA in their day to day lives. Future work could explore how to document these harms in a more

systematic manner, perhaps through quantitatve measurements. While not all harms can be easily quantified, it can be helpful to measure and make public harms that *are* quantifiable.

For example, one disruptive characteristic about OBA that participants brought up was the sheer amount of ads they saw. One first step toward concretizing this as a harm is to record the number of ads shown and how much time and data they take to load. Popular ad and cookie blockers (e.g., PrivacyBadger[2], uBlock Origin[3]) already show counts of trackers and ads found and blocked during a user's browsing experience. The Brave browser, which also blocks ads, goes one step further, calculating the amount of time and bandwidth it would have potentially taken to load them if they were not blocked; these metrics are displayed to users as bandwidth and hours "saved", purportedly analogous to 23 USD per month per user[4]. Beyond automatically measurable variables like ads blocked, we can envision third-party watchdogs (e.g., EFF, Consumer Reports) developing tools that help users collectively report on ads or ad practices that distress, constrict, and marginalize. Empirically and explicitly measuring all the different OBA harms we uncovered in this work, aggregated over a "sufficiently substantial" number of users, could present compelling evidence to government officials of a privacy harm.

5.2.2 Documentation of evasive action. Ashley Gorski, a staff attorney at the American Civil Liberties Union (ACLU), has argued that it is often easier to "produce evidence of protective measures than evidence of secret surveillance itself" [21]. When people stop using devices or software, or switch to sub-optimal services to avoid surveillance, they are taking actions that cost them; thus, as Gorski contends, they are being injured by that amount of time and money. In other words, actions that users have taken *against* OBA could qualify as an injury, evoking our "constriction of user behavior" harm type. Different evasive actions might also help signal the other OBA harm types we uncovered: for example, users who provide false information about themselves might wish to avoid algorithmic marginalization, whereas those who disable their smart home device microphones may wish to avoid the psychological distress of being constantly surveilled. Thus—concurrent with documenting harms generally—measuring the amount of time, money, effort, and other resources that users take to *avoid* OBA is another form of evidence for courts and legislative figures.

5.3 Limitations

Our work has a few limitations. For one, our participant pool was entirely located in the United States of America, limiting the cultural scope and policy relevance of our findings. Another limitation is the use of Prolific for recruitment: while some past work has found that users on Amazon Mechanical Turk (MTurk), a similar crowdwork platform, were fairly representative of the U.S. population in S&P experiences and education [36], other work has found that they have higher privacy concerns and were better-educated about S&P than the larger U.S. public [26]. Future work could explore the extent to which users from different cultural and regulatory contexts—e.g., more collectivist countries [35], or the European Union, where the GDPR strictly enforces user consent—as well as different educational backgrounds, might hold different attitudes regarding what is harmful.

[2]https://privacybadger.org/
[3]https://ublockorigin.com/
[4]https://brave.com/tips-and-tricks-for-brave-on-your-phone/

6 CONCLUSION

Online behavioral advertising is a key driver of surveillance capitalism [49], which has resulted people feeling concerned about the state of privacy but helpless to effect change [6]. The first step in empowering people is to provide a model and vocabulary for the many ways online behavioral advertising harms people. In this paper, we provide this model of lived OBA harms. Through a survey of 420 participants online, we uncovered four key types of harms that users endure from OBA: psychological distress, loss of autonomy, constriction of user behavior, and algorithmic marginalization and traumatization. We then discussed how users can become inured to these harms over time, and how formal legal recognition of these harms can be a first step to mitigating them. Finally, we recommend that FAccT, HCI, and privacy researchers reconceptualize OBA as part of a bigger picture of privacy-encroaching, actively harmful societal practices, and provide initial guidance for how we might combat and mitigate these practices.

ACKNOWLEDGMENTS

Dr. Peter Swire, at Georgia Institute of Technology, was instrumental in helping us contextualize how our work might relate to ongoing discussion among legal scholars about the standing and recognition of privacy harms.

REFERENCES

[1] 2016. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549.
[2] 2019. Harm. In *Black's Law Dictionary*, Brian A Garner (Ed.). Thomson Reuters.
[3] 2021. TransUnion LLC v. Ramirez, 141 S. Ct. 2190.
[4] Muhammad Ali, Piotr Sapiezynski, Miranda Bogen, Aleksandra Korolova, Alan Mislove, and Aaron Rieke. 2019. Discrimination through optimization: How Facebook's Ad delivery can lead to biased outcomes. *Proceedings of the ACM on human-computer interaction* 3, CSCW (2019), 1–30.
[5] Micah Altman, Alexandra Wood, and Effy Vayena. 2018. A harm-reduction framework for algorithmic fairness. *IEEE Security & Privacy* 16, 3 (2018), 34–45.
[6] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. (2019).
[7] Tae Hyun Baek and Mariko Morimoto. 2012. Stay away from me. *Journal of advertising* 41, 1 (2012), 59–76.
[8] Dylan Baker, Alex Hanna, and Emily Denton. 2020. Algorithmically encoded identities: reframing human classification. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 681–681.
[9] Colin J Bennett and Jesse Gordon. 2021. Understanding the "Micro" in Political Micro-Targeting: An Analysis of Facebook Digital Advertising in the 2019 Federal Canadian Election. *Canadian Journal of Communication* 46, 3 (2021), 431–459.
[10] Colin J Bennett and David Lyon. 2019. Data-driven elections: Implications and challenges for democratic societies. *Internet Policy Review* 8, 4 (2019).
[11] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science* 4, 3 (2013), 340–347.
[12] Ryan Calo. 2011. The boundaries of privacy harm. *Ind. LJ* 86 (2011), 1131.
[13] Stevie Chancellor, Michael L Birnbaum, Eric D Caine, Vincent MB Silenzio, and Munmun De Choudhury. 2019. A taxonomy of ethical tensions in inferring mental health states from social media. In *Proceedings of the conference on fairness, accountability, and transparency*. 79–88.
[14] Stevie Chancellor, Shion Guha, Jofish Kaye, Jen King, Niloufar Salehi, Sarita Schoenebeck, and Elizabeth Stowell. 2019. The relationships between data, power, and justice in cscw research. In *Conference Companion Publication of the 2019 on Computer Supported Cooperative Work and Social Computing*. 102–105.
[15] Danielle Keats Citron and Daniel J Solove. 2022. Privacy harms. *BUL Rev.* 102 (2022), 793.

[16] Sauvik Das, Cori Faklaris, Jason I Hong, Laura A Dabbish, et al. 2022. The Security & Privacy Acceptance Framework (SPAF). *Foundations and Trends® in Privacy and Security* 5, 1-2 (2022), 1–143.

[17] Jenny L Davis and Nathan Jurgenson. 2014. Context collapse: Theorizing context collusions and collisions. *Information, communication & society* 17, 4 (2014), 476–485.

[18] Federal Trade Commission. 2009. *FTC Staff Report: Self-regulatory principles for online behavioral advertising*. Technical Report. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-staff-report-self-regulatory-principles-online-behavioral-advertising/p085400behavadreport.pdf

[19] Steven Furnell and Kerry-Lynn Thomson. 2009. Recognising and addressing 'security fatigue'. *Computer Fraud & Security* 2009, 11 (2009), 7–11.

[20] Liza Gak, Seyi Olojo, and Niloufar Salehi. 2022. The Distressing Ads That Persist: Uncovering The Harms of Targeted Weight-Loss Ads Among Users with Histories of Disordered Eating. *arXiv preprint arXiv:2204.03200* (2022).

[21] Ashley Gorski. 2022. The Biden Administration's SIGINT Executive Order, part II. https://www.justsecurity.org/83927/the-biden-administrations-sigint-executive-order-part-ii/

[22] Julia Hanson, Miranda Wei, Sophie Veys, Matthew Kugler, Lior Strahilevitz, and Blase Ur. 2020. Taking Data Out of Context to Hyper-Personalize Ads: Crowdworkers' Privacy Perceptions and Decisions to Disclose Private Information. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–13.

[23] Cormac Herley. 2009. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*. 133–144.

[24] Cormac Herley. 2016. Unfalsifiability of security claims. *Proceedings of the National Academy of Sciences* 113, 23 (2016), 6415–6420.

[25] Carlos Jensen and Colin Potts. 2004. Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. 471–478.

[26] Ruogu Kang, Stephanie Brown, Laura Dabbish, and Sara Kiesler. 2014. Privacy attitudes of mechanical turk workers and the us public. In *Symposium on Usable Privacy and Security (SOUPS)*, Vol. 4. 1.

[27] Hao-Ping Lee, Jacob Logas, Stephanie Yang, Zhouyu Li, Nata Barbosa, Yang Wang, and Sauvik Das. 2022. When and Why Do People Want Ad Targeting Explanations? Evidence from a Four-Week, Mixed-Methods Field Study. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 923–940.

[28] Aleecia M McDonald and Lorrie Faith Cranor. 2009. The Cost of Reading Privacy Policies 2008 Privacy Year in Review. I. *S: A Journal of Law and Policy for the Information Society* 4, 3 (2009), 2008.

[29] Silvia Milano, Brent Mittelstadt, Sandra Wachter, and Christopher Russell. 2021. Epistemic fragmentation poses a threat to the governance of online targeting. *Nature Machine Intelligence* 3, 6 (2021), 466–472.

[30] George R Milne, Mary J Culnan, and Henry Greene. 2006. A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing* 25, 2 (2006), 238–249.

[31] Jared Moore. 2020. Towards a more representative politics in the ethics of computer science. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. 414–424.

[32] Rob Nixon. 2011. *Slow Violence and the Environmentalism of the Poor*. Harvard University Press.

[33] Chris Norval, Kristin Cornelius, Jennifer Cobbe, and Jatinder Singh. 2022. Disclosure by Design: Designing information disclosures to support meaningful transparency and accountability. In *2022 ACM Conference on Fairness, Accountability, and Transparency*. 679–690.

[34] Elleen Pan, Jingjing Ren, Martina Lindorfer, Christo Wilson, and David R Choffnes. 2018. Panoptispy: Characterizing audio and video exfiltration from android applications. *Proc. Priv. Enhancing Technol.* 2018, 4 (2018), 33–50.

[35] Elissa M Redmiles. 2019. " Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 920–934.

[36] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.

[37] John S Seberger, Marissel Llavore, Nicholas Nye Wyant, Irina Shklovski, and Sameer Patil. 2021. Empowering resignation: There's an app for that. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–18.

[38] John S Seberger, Irina Shklovski, Emily Swiatek, and Sameer Patil. 2022. Still creepy after all these years: the normalization of affective discomfort in app use. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–19.

[39] Edith G Smit, Guda Van Noort, and Hilde AM Voorveld. 2014. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in human behavior* 32 (2014), 15–22.

[40] Daniel J Solove. 2012. Introduction: Privacy self-management and the consent dilemma. *Harv. L. Rev.* 126 (2012), 1880.

[41] Daniel J Solove and Danielle Keats Citron. 2021. Standing and Privacy Harms: A Critique of TransUnion v. Ramirez. *BUL Rev. Online* 101 (2021), 62.

[42] Joseph Turow, Michael X Delli Carpini, Nora A Draper, and Rowan Howard-Williams. 2012. Americans roundly reject tailored political advertising. (2012).

[43] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, useful, scary, creepy: perceptions of online behavioral advertising. In *proceedings of the eighth symposium on usable privacy and security*. 1–15.

[44] Miranda Wei, Madison Stamos, Sophie Veys, Nathan Reitinger, Justin Goodman, Margot Herman, Dorota Filipczuk, Ben Weinshel, Michelle L Mazurek, and Blase Ur. 2020. What twitter knows: characterizing ad targeting practices, user perceptions, and ad explanations through users' own twitter data. In *Proceedings of the 29th USENIX Conference on Security Symposium*. 145–162.

[45] Ben Weinshel, Miranda Wei, Mainack Mondal, Euirim Choi, Shawn Shan, Claire Dolin, Michelle L Mazurek, and Blase Ur. 2019. Oh, the places you've been! User reactions to longitudinal transparency about third-party web tracking and inferencing. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 149–166.

[46] Yuxi Wu, W Keith Edwards, and Sauvik Das. 2022. "A Reasonable Thing to Ask For": Towards a Unified Voice in Privacy Collective Action. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. 1–17.

[47] Yaxing Yao, Davide Lo Re, and Yang Wang. 2017. Folk models of online behavioral advertising. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*. 1957–1969.

[48] Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2021. What makes a "bad" ad? user perceptions of problematic online advertising. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–24.

[49] Shoshana Zuboff. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power: Barack Obama's books of 2019*. Profile books.

[50] Shoshana Zuboff. 2019. Surveillance capitalism and the challenge of collective action. In *New labor forum*, Vol. 28. SAGE Publications Sage CA: Los Angeles, CA, 10–29.

A CODEBOOK

Initial Category	Label
Emotional reactions	distrust in institutions
	feeling like I didn't consent
	frustrated, annoyed
	I'm already proactive about privacy
	invaded
	overwhelmed by number of ads
	paranoid
	surprised
	unsettled, uncomfortable
Emotional/psychological changes	changed perception of advertiser
	feeling effects on mental health
	feeling like my thoughts are being predicted
	influenced my purchasing behavior
	knowing mics are not on but still feels like it
	made me more proactive about privacy
	wanting to guess at how ads got their data
	work/personal life crossover
Physical actions	blocking future ads
	deleting app/service/account
	disabling voice assistant
	stop having conversations near device
	stop using app/service/account
Ad content origin guesses	my demographics
	my location data
	my physical/IRL purchases
	my searches/browsing
	my smart home devices
	talking out loud/mic usage
	talking on social media
Sensitive or offensive content	ad contains misinfo/scam
	ad refers to someone else's shopping
	generally sensitive content
	generally hurtful/offensive content
	incorrect targeting
	medical/health ad: general
	medical/health ad: mental health

Table 3: Codebook used in analysis of survey responses. The left column, "Initial Category", refers to non-prescriptive categories we used as references in early discussions of the data. These groupings loosely formed a basis for the typology of harms.