"I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country

Kovila P.L. Coopamootoo and Maryam Mehrnezhad, *Newcastle University;*
Ehsan Toreini, *Durham University*

https://www.usenix.org/conference/usenixsecurity22/presentation/coopamootoo

This paper is included in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

"I feel invaded, annoyed, anxious and I may protect myself": Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country

Kovila P.L. Coopamootoo
Newcastle University, UK
kovila.coopamootoo@newcastle.ac.uk

Maryam Mehrnezhad
Newcastle University, UK
maryam.mehrnezhad@newcastle.ac.uk

Ehsan Toreini
Durham University, UK
ehsan.toreini@durham.ac.uk

Abstract

Online tracking is a primary concern for Internet users, yet previous research has not found a clear link between the cognitive understanding of tracking and protective actions. We postulate that protective behaviour follows affective evaluation of tracking. We conducted an online study, with N=614 participants, across the UK, Germany and France, to investigate how users feel about third-party tracking and what protective actions they take. We found that most participants' feelings about tracking were negative, described as deeply intrusive - beyond the informational sphere, including feelings of annoyance and anxiety, that predict protective actions. We also observed indications of a '*privacy gender gap*', where women feel more negatively about tracking, yet are less likely to take protective actions, compared to men. And less UK individuals report negative feelings and protective actions, compared to those from Germany and France. This paper contributes insights into the affective evaluation of privacy threats and how it predicts protective behaviour. It also provides a discussion on the implications of these findings for various stakeholders, make recommendations and outline avenues for future work.

1 Introduction

In recent years, internet advertising has become increasingly tailored to individual users, and is often referred to as online behavioural advertising or targeted advertising [25]. When users visit a web page, its contents can come from a first- or third-party, where the first-party is the one the user is explicitly visiting, while the third-party includes advertising networks, analytics companies and social networks that contract with first-party websites [43]. The first- or third-party places cookies as tracking mechanism on users' devices. In addition, online tracking has gradually developed into more sophisticated methods to exploit user data, via browser-based fingerprinting [52] and tracking across multiple devices, where fingerprinting information combined with cookies can provide a well-targeted data collection and tracking of users. Other tracking technologies include web beacons, clear GIFs, page tags and web bugs, that take the form of a small, transparent image. In European countries, the General Data Protection Regulation (GDPR) [67] and the proposed ePrivacy Regulation [18], with the UK establishing its implementation [49], stipulate that online service providers are required to inform individuals that tracking technologies are present, what they do and why, and to receive users' consent to use them.

The general public opinion in national surveys as reported in the UK and Europe is that tracking online is a privacy concern for most citizens [10, 16], and objecting to receiving direct marketing is the most exercised right in Europe (accounting for 24% of participants surveyed in 2019) [17]. However, research shows that individuals have inaccurate and incomplete mental models of the mechanics of behavioural advertising [78] and have misconceptions about the purpose of cookies [44]. They perceive behavioural advertising to be either (or simultaneously) useful in providing ads that match their interests [5, 44, 71], privacy-invasive [44, 70, 71], creepy [71], embarrassing or suggestive [1], and often show varying acceptance of behavioural advertising depending on the context [12, 45, 72]. With regards to the use of privacy technologies for tracking protection, users' mental models of tracking (that is their cognitive evaluation of tracking) only weakly relate to their use of tracker-blocking extensions [42], where tracking protection tools are also thought to suffer from usability issues [23, 37, 59].

We postulate instead that *affective evaluations* can better predict protective actions. We ground our proposition in literature on the informative and decisive value of emotions, where models such as the affect-as-information hypothesis [15], the risk-as-feelings hypothesis [40], or the use of affective heuristics when judging risky situations [63], all explain the influence of affect in decisions and on behaviour.

In addition to all Internet users potentially facing threats to their privacy, demographic and personal attributes may influence the experience of tracking and protective behaviour. In particular, it is known that women tend to be more sensi-

tive and concerned about their privacy online compared to men [11, 46], who have been shown to be more familiar with various privacy protection methods and to use them more often than women [46]. Furthermore, individuals of different countries may use different privacy protection practices [19], where variation in behaviour may be due to differences in the importance attributed to data protection [64], in sensitivity with regards to the duration or quantity of data collected [21] or in the perceived risks of privacy violations [35].

As a consequence, we aim to investigate how feelings about (third-party) tracking associate with and predict protective behaviour, across gender and country. To enable this inquiry, we define the following research questions, starting with elicitation of feelings and protective actions:

RQ1 "*How do individuals feel with regards to third-party tracking?*", given their gender and country differences.

RQ2 "*What tracking protective actions do individuals employ online?*", given their gender and country differences.

RQ3: "*How are individuals' feelings about third-party tracking associated with their protective actions?*"

RQ4: "*How do individuals' feelings about third-party tracking predict whether they take protective actions or not, given their gender and country differences?*"

Contributions. This paper contributes a relatively large-scale, gender-based and cross-national investigation of user tracking protection, to the rich user-centric privacy behaviour and tracking protection research area. It employs qualitative and quantitative analyses to answer the research questions. We summarise our findings as follows:

(1) most individuals (71.8% of our sample) feel negatively about third-party tracking, where feeling tones can be broadly categorised into (a) generally not okay/negative, (b) sometimes okay, sometimes not okay, (c) generally okay/indifferent, or (d) other tones;

(2) individuals employ tracking protection actions that can be grouped within 9 technology types and a relatively large % do not take any protective actions (34.7% of our sample);

(3) there is a significant association between feelings about third-party tracking and self-reported actions, and we provide an intuitive spatial map to visualise this association;

(4) feeling tones of not okay, boundary loss, annoyance or anxiety about tracking predict whether individuals take protective actions or not;

(5) more women feel negatively about tracking and report to not take any protective actions, compared to men, whose reports show that they are twice more likely to act protectively than women;

(6) less UK individuals expressed negative feelings and reported protective actions, compared to German and French individuals. UK individuals were also twice less likely to take any protective actions.

Outline. In the rest of the paper, we review relevant literature, present the user study with the method and results, discuss the implications of our findings and conclude.

2 Background

We review literature on user attitudes, perceptions and protection methods with regards to tracking. We then present research supporting the affective aspects of privacy, and review theories and research on behavioural responses to emotions. We complete this section with gender and national culture impacts on privacy.

2.1 Tracking Attitudes, Understanding & Protective Behaviour

Individuals perceive behavioural advertising to be privacy-invasive [44, 70, 71]. In particular, individuals (1) do not want third parties to track and profile them online [54], (2) are particularly concerned about the amount of data, the presence of sensitive information, and the data from offline sources found in tracked profiles [54], (3) are sensitive to embarassing ads [1], (4) are concerned about the lack of transparency and control over behavioural advertising practices [71], (5) are concerned that tracking could possibly lead to disadvantages in real life, and do not trust tracking [68]. However, individuals also perceive behavioural advertising to be useful in providing ads that match their interests [5, 44, 71], enjoy its informativeness and utility for making purchasing decisions [60], feel comfortable in specific situations [45], and show varying acceptance of behavioural advertising depending on the context [12, 45, 72]. In addition, research shows that individuals have basic understanding of online tracking [42] and inaccurate and incomplete mental models of the mechanics of behavioural advertising, such as conceptualising trackers as viruses that access local files and reside on the local computer [78], and having misconceptions about the purpose of cookies [44]. With regards to protective behaviour, users want more control over tracking and perceive the benefits of controlled tracking, but are unwilling to put in the effort to control tracking, distrust existing tools [45] or have limited awareness of the of countermeasures and how to use them [62], while some have reported to protect from tracking [52].

2.2 The Affective Aspects of Privacy

Although emotions are an integral aspect of decision-making and behavior, research into emotional context of privacy is relatively new, and privacy decision-making has mainly been treated as a cognitive process. A limited number of research have demonstrated and argued that the emotional aspect of privacy is as important [27, 65], including (1) FMRI neurobiological research providing evidence that privacy decisions are found to be in the more affective-cognitive area of the human brain than purely cognitive [27]; (2) research in the affective dimension of privacy attitude [20]; (3) privacy decision-making research on the role of affect in disclosing personal

information [39], in subconsciously shaping privacy risk perceptions [32] or overriding rational factors [34]; (4) research on the influence of discrete emotions (such as anger, anxiety, fear, regret) in leading to problem- and emotion-focused privacy coping strategies [13]; as well as (5) HCI research on the influence of emotional valence in interfaces on privacy concerns [33]. These are supported by arguments from scholars who advocate for a greater attention to the phenomenology of feeling and to the concept of "visceral" design in information privacy scholarship, policy, and design practice [65].

2.3 Behavioural Response to Emotions

It is universally agreed that affect influences individuals' decisions, where human beings go through both cognitive and affective responses to stimuli. While cognitive responses indicate individuals' mental process in interaction with the stimuli, their affective responses designate individuals' emotional feedback from environmental cues. Several models such as the affect-as-information hypothesis [15], the risk-as-feelings hypothesis [40], or the use of affective heuristics when judging risky situations [63], all explain the influence of affect in decisions and on behaviour.

Affective evaluations are thought to reflect and translate the cognition of (privacy) concern or risk, leading to *coping behaviour* [8], where coping is defined as an individual's efforts to manage stressful, aversive or disruptive events [36]. This is inline with the protection motivation theory that describes how individuals are motivated to react in self-protective ways towards a perceived threat and to adopt coping strategies [76].

The couple of research into users' responses to affective privacy evaluations have investigated emotions associated with privacy risks and their resulting emotional coping (such as acceptance, avoidance, disengagement, or venting [13,31]), active problem-solving (such as company complaints [31], negative-word-of-mouth [47], decreased usage time [47]) or protective actions (such as engaging with privacy settings [31]), in contexts such as location-based services [31], social networks [13], and smart speakers [47]. They focused on negative emotions [13,31,47], such as anger, frustration, disappointment, anxiety, fear and regret, with the assumption that, as privacy loss and privacy risks contexts are generally considered as aversive rather than appetitive (or approach), they are more likely to elicit negative reactions than positive reactions [20].

2.4 Demographic Influence of Privacy

Women tend to be more concerned about their general privacy [7,61,75,79], as well as privacy with regards to specific technology (such as mobile devices [58] and online advertising [61]), compared to men. However, there are nuances in response to concerns for men versus women, with regards to protective behaviour. Women have been found to be less confident and less equipped with technical skills to manage personal data [48], and more likely to use avoidance behaviours such as limiting the sharing of sensitive information [55], while men have been found to be more familiar with the privacy protection strategies and to use them more often [46]. However women are thought to be as apt as men in social privacy protection strategies [48,79], such as taking protective actions in social network sites [9] or refraining from using websites that ask for personal information [79].

This distinction in concern and protective behaviour between women and men brings into focus the feminist perspectives of privacy [2,41], where women are thought to not enjoy the same level and types of desirable privacy online as men. The conceptions of public/private spheres are thought to render women vulnerable, where they may have too much of the 'wrong' kind of privacy, where a rigid binary classification of women versus men and surveillance also perpetuate patriarchal systems at the detriment of women, who are significantly identified and revealed but do not have agency in expressing and exercising their privacy.

National culture, as the collective mindset distinguishing members of one nation from another [29], also influences privacy concern, behaviour or valuation of information [14, 57, 69]. Between the UK and Europe, there are indications of the British exhibiting different privacy technology usage behaviour compared to other countries, where in contrast, German users are thought to be better versed with 'advanced' privacy technologies [19]. Compared to other countries (US or EU), German nationals attribute a higher importance to data protection [64], in sensitivity of data collected [21] or in the perceived risks of privacy violations [35].

3 Related Research & Gaps

In this section we compare our contributions to the most closely related previous research.

User-centred aspects of tracking: Previous research has mostly inquired into the cognitive dimension of tracking, such as via user perceptions [44, 70, 71, 78], attitudes [60] and concerns [54, 77] of online behavioural advertising for insights into tracking. A few investigations have focused their elicitation methods particularly towards tracking perception and mental model [12,42,62], concerns [1], preferences [45], or third-party tracking online [68].

While feelings with regards to tracking have come up in investigations of perceptions and concerns about behavioural advertising and tracking (such as 'creepy' or 'scary') [71], to our knowledge, previous research has not explicitly asked individuals how they *felt* about third-party tracking, that is, with an intention to specifically elicit feeling tones. This current research explicitly investigates feeling tones with an intention to map these with protective actions.

For protective behaviour related to tracking, research has qualitatively elicited protective actions and the use of privacy

technologies in general [12, 52, 62], or queried use of specific technologies such as browser extensions [42]. We use an open-ended method to elicit individuals' protective actions.

Behavioural Response to Affective Privacy Evaluation: Previous studies [13, 31] have focused on technology contexts that are different to this paper, as reviewed in Section 2.3. In addition, these studies query participants to a preset list of discrete negative emotions and coping behaviours, whereas we extract feeling tones and protective actions from participants' free form response.

4 Method

In this section we provide details about participant recruitment and characteristics, the study procedure and questionnaire design, the research ethics process, as well as the design limitations.

4.1 Participants

We recruited participants via Prolific Academic, a crowdsourcing platform whose data quality has good reproducibility [50] is comparable to Amazon Mechanical Turk's which is widely used within security and privacy user studies. The study lasted between 20 to 30 minutes. Participants were compensated at a rate of £7.5 per hour, slightly above the minimum rate of £5 per hour, as advised by Prolific Academic.

We sampled around 630 participants and ended with $N = 614$ after removing incomplete attempts at the survey. The study was balanced by number of participants in each country and gender. The $N = 614$ participants consisted of $n = 209$ from the United Kingdom (UK), $n = 202$ from Germany (GE) and $n = 203$ France (FR). We chose these three countries as they have the highest number of internet users in Europe [66] and therefore a high number of users potentially exposed to online tracking. While nationals of different countries, such as the UK, Germany and France, may exhibit different privacy behaviour [19], we note that the UK has similar data protection provisions as the rest of Europe, as it has established its implementation of the GDPR, where the principles, rights and obligations of the 'UK GDPR' follows the European one [49]. Overall there was approximately a similar number of women ($n = 307$) and men ($n = 299$) participants (about 100 each in each country) and 8 self-reporting as non-binary. The rationale for balancing across gender is that women may engage in different protection practices compared to men, who are known to be more familiar with protection methods [48]. Women can be considered as a vulnerable user group, where as explained by the 'differential vulnerabilities' concept that recognizes how different populations face different types and degrees of security and privacy risks [51], they may experience more harmful impact from the same online threats, compared to men. We posit that such user groups need dedicated research and support.

Table 1: Participant Characteristics

Country	*N*	**Mean Age**	**Gender**		
			#F	#M	#N
United Kingdom	209	35.78	109	100	0
Germany	202	29.21	100	100	2
France	203	27.29	98	99	6
Education	*%*	**Ethnicity**	*%*	**Most Used Browsers**	*%*
High School/lower	26.1	white	86.6	IE	10.4
College	17.6	mixed	5.0	Chrome	72.3
Undergraduate	29.0	asian	4.1	Firefox	34.0
Masters	24.9	black	2.1	Safari	19.4
Phd	2.2	other	2.1	Opera	5.7
				Brave	9.4
				Other	6.7

Table 1 provides a summary of the demographic details. The table also lists the most used browsers, where 'other' included mentions of DuckDuckGo, Tor, Microsoft Edge, Chromium or Vivaldi.

4.2 Procedure

We ran the study as an online survey during 2020. Participants were first presented with (1) a consent form (as described in Section 4.3 below), (2) followed with a demographics questionnaire, (3) elicitation of their feelings with respect to tracking online, and (4) their own protective actions. The survey was proof-read by the authors, and 3 of their acquaintances who are not experts in the topic. In addition, the survey was piloted on Prolific Academic across the three countries, where we invited 9 pilot participants, with 95% approval rate, to comment on the survey, thereby facilitating enhancements.

The first page of the survey gave information about the study, letting participants know that the study was anonymous, that participation was voluntary, and explicitly asked for opt-in consent for participation.

Next, we describe the feelings and protective actions elicitation, as well as provide the questions verbatim. These were set as open-ended questions with participants responding in free-form text. ***Feelings:*** To bring participants' own experience and feelings about tracking to the fore, we used a method similar to a mood induction protocol [74] to elicit feelings about an issue. We first asked participants to write about their understanding of third-party tracking as a way of inducing their mental picture of third-party tracking. We then asked them to express their feelings about third-party tracking on the web in their words, in writing. The two questions were set as: (1) "*In your own words, write about your own understanding of third-party tracking on the web. In particular, what does third-party tracking mean?"* followed with (2) "*How do you feel with regards to third-party tracking on the web. Please name emotions and/or perceptions if relevant. With regards to third-party tracking, I feel ...* ". Note that we focus

on feeling tones, rather than traditional measures of emotions or affect [73], because we aim to investigate the mood or feeling associated with the particular experience (or stimulus) of tracking (inline with APA dictionary's definition of feeling/affective tone [3]).

Protective Actions: We followed with a question to elicit participants' tracking protection actions, where we asked them to name the actions they employ. In particular, we asked "*What actions have you taken to protect yourself from tracking (including third-party tracking), as you browse the web?*".

After data collection, incomplete attempts at the survey, making up 16 participants, were removed leaving us with $N = 614$ participants. We then progressed into qualitative analysis of the free-form responses to the feelings and actions questions. We provide description of this analysis, including the creation of a codebook, in Section 5. We used these codes to report on feeling tones and actions, across gender and country, as well as within the quantitative analyses that follow. We summarise the study design in Figure 1.

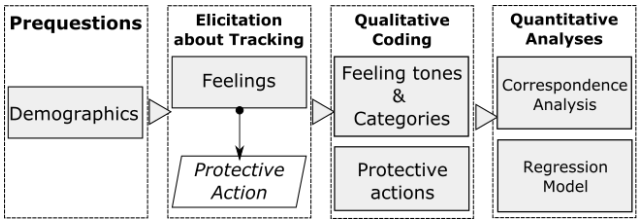

Figure 1: Study design

4.3 Ethics

We obtained full approval from Newcastle University's Ethics Committee before the research commenced. We also sought participants' opt-in consent for data collection prior to their responding to the questionnaire. In addition to having undergone independent ethical review, we designed our user studies to address pillars of responsible research in computer science [6]. Participation in the study was voluntary and anonymous and our participants could drop out of it at any stage.

4.4 Limitations

We discuss the limitations of the study design as follows.

We queried protective actions in participants' own words, which assumes at least a minimum awareness and understanding of the actions they employ, rather than providing a predefined list of privacy technologies for participants to choose from. However, we specifically queried participants on protective actions and did not capture other behaviours that they may employ for emotional coping, as described in Section 2.3.

The study relies mainly on self-reports, which is a widely used and valuable form of eliciting user responses in privacy and security user studies. While self-report can be argued to induce bias, previous research has also found that self-report insights can translate to real-world settings [56]. In addition, free-form responses provide a rich view of users' own experience.

By choosing to position the demographics questionnaire at the beginning of the survey, the study may have been affected by 'stereotype threats' [30]. We would therefore opt for a different placement of demographic questions in the future.

Although the study was piloted across the countries, it was written in English, and therefore has minor limitations on who can take the survey. Future studies targeting different nationals across countries may consider using their first language.

Because the number of non-binary participants was only 8, our gender comparisons and statistical analyses focus on women versus men. We hope to target a more diverse sample in future research. In addition, while other user characteristics (such as skills) may affect experience and protective actions, we focused and balanced our sample on gender and country demographics. A future study may compare the influence of a further list of user characteristics. Furthermore, although having a relatively large-scale qualitative grounding, the study was directed at the UK and European countries, thereby limiting generalisability to other national cultures.

5 Qualitative Coding

In this section, we describe our process of extracting participants' feeling tones and actions from their responses.

5.1 Feeling Tones

Identification of Themes & Codebook Creation. We looked into participants' free-form text responses.We used a conventional line-by-line coding method (as previously employed in user-centric privacy research [20]), where we read each response and identified specific themes. We know from previous research that individuals find tracking to be worrisome (scary [71]), embarassing [1], have mixed feelings about tracking [12,45,72] or are okay with tracking [44,71]. We therefore sought to identify whether participants were in general, (1) okay or do not care about tracking, (2) not-okay or feel negatively (3) sometimes okay, sometimes not-okay or okay under certain conditions. We further looked into the emotions and/or reasoning expressed by participants, and also identified 'other' themes that were not categorised in the three categories. We note that while some participants only expressed how they felt about tracking, most participants provided a reasoning in association to their feelings. We detail these in the results Section 6.1. We summarise the feeling tones according to their categories, as well as the % participant responses that express them, in Table 2. We also provide the whole codebook with example words in Appendix A in Table 5.

Coder Reliability. One researcher created the codebook, which was then provided to a second researcher along with

Table 2: Categories and Example Tones (N=614)

Tone Category	Feeling Tone	% Participants
Generally not okay (Negative)	Not_Okay	4.6
	Boundary_loss	17.8
	Unfair	8.6
	Annoyance	12.5
	Anxiety	12.4
	Discomfort	9.1
	Distrust	3.9
Sometimes okay, sometimes not okay	Ambivalent	7.7
	Okay_if	2.9
	Okay_ protected	2.3
Generally okay / indifferent	Okay	4.7
	Indifferent	2.9
	Necessity	0.7
	None	1.6
Other	Should_regulate	2.9
	Not_aware	5.4

a sample of responses. The codebook was iteratively refined, after which two researchers coded the whole set of responses. We computed 95% agreement between coders as well as Cohen k of .820, $p < .001$, suggesting substantial agreement in applying the codebook.

5.2 Protective Actions

We used a line-by-line coding to extract words such as 'browser option', 'extension' or specific names for privacy-enhancing technology (PET) such as 'Ublock', and categorised these into tracking protection methods. Because the coding involved simply identifying specific words relating to tracking protection, it was conducted by one researcher only. Participants also mentioned strategies that we grouped under '**other**'. These included actions such as 'checking social media settings or avoiding public Wi-Fi. We describe these in Section 6.2. We summarise the protective actions by % participants naming them in Table 3. Note that some participants named more than one protective action.

Table 3: Protective Actions (N=614)

Actions	% Participants
extension	27.7
clear cookies	16.6
private browsing	13.5
VPN	11.1
builtin browser setting	9.6
clear browser history	3.3
anti-malware, -virus	2.6
safe website	2.1
other	8.0
No Action	34.7

6 Results

We report our qualitative and quantitative findings. We note that for gender-based comparisons, to aid statistical reporting, we focus on male versus women only, as only 8 out of 614 participants self-reported as non-binary.

6.1 Feelings about Third-Party Tracking

We investigate RQ1, that is "How do individuals feel with regards to third-party tracking?", given their gender and country differences. We summarised the feeling tones extracted from participants' responses and their categories in Table 2. In the following subsections, we (1) provide the % of participants expressing the feelings in each category, across gender and country and then we (2) describe the extracted feeling tones, while providing example responses from participants. In the example responses, we refer to UK participants as UK#, German participants as GE# and French participants as FR#.

6.1.1 Generally Not Okay (Negative Feelings)

Participants' whose feeling tones were in congruence with not being okay with third-party tracking (referred to as TPT in the results section) either just said so, named (their concern with respect to) the threats of TPT (such as invaded privacy or self/boundary loss, unfair practice by others) or went further to describe their emotional response as a result of TPT (such as anger, anxiety, distrust or discomfort).

Figure 2 summarises the feelings tones categorised under generally not okay or negative feelings. We notice patterns across gender and country, for example that (1) more women expressed negative feelings in all countries; (2) less UK participants expressed negative feelings compared to Germany and France, across both gender; and (3) slightly more men expressed the mix of feelings till 'annoyance', but more women expressed 'anxiety, discomfort, distrust' (combined).

Not Okay: 4.6% of participants said they were not okay with TPT, such as by saying that they did not feel good about TPT (without mentioning particular emotions), or clearly stating that they do not like or want TPT and are against TPT. Example responses include: GE179 "***I do not feel very good about it**, because I don't know where my data will end up*", UK20 "***I don't like it** and I don't like other companies having my information*", FR116 "*If they're what i think they are, then **i really don't like this business model** [sic]*", UK114 "***I dislike that you have to actively log out of offering this access to third parties**...*", FR113 "***opposed***", UK164 "***I am strongly against** unannounced third party tracking...*", and FR128 "***I would rather not be tracked at all***".

Boundary loss and invasion: 17.8% participants described feeling an invasion or violation with regards to their online privacy, such as expressed by UK36, "*That it is an **invasion of your personal details** and that keeping it to just*

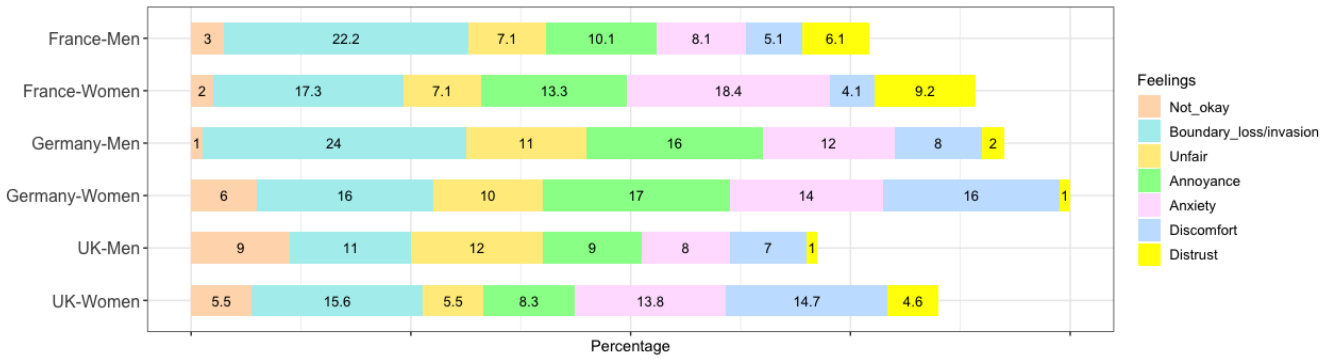

Figure 2: *Negative* feelings expressed across gender & countries (the x-axis shows % in each gender-country group with n=100 approx.) *See text for description of noticeable patterns, such as more women feel negatively & less UK participants feel negatively.*

those companies that you choose to deal with would be ideal but you know that info will probably end up being passed on...", by UK85 "*this is a* ***violation of privacy and of freedom***", or UK90 "*An invasion of privacy, masqueraded by third party/flimsy data protection rules*".

This feeling tone also included participants who went further to express how they felt with regards to the loss of boundaries, in particular noting the consequences to their personal sphere or sense of self, such as expressed by GE1 "*With regards to third-party tracking, I feel* ***exposed*** *to the web*", UK68 "*slightly out in the open*", UK51 "*I feel* ***violated*** *and as though my privacy and security is not respected*". GE25 "***unsecure*** *since I value my privacy. I don't want third partys [sic] to get access to any of my personal information*, GE27 "*exposed,* ***exploited***", GE66 "***unsafe****, spied on*", GE134 "*I feel like my every move is being* ***monitored***", and UK115 "*I don't like the idea of being* ***stalked*** *online, however that may be*".

Additionally, some participants from Germany and France used even stronger wordings to describe feeling deeply invaded as a person, or dis-humanised, such as GE7 "*unsafe. I feel* ***naked.*** *'transparent human' we call that in German [sic]. I feel like nothing is private anymore, even if I seek the anonymity of the internet for a reason*", FR4 "*I feel* ***raped****, robbed, angry*", FR143 "*I feel this is very* ***intrusive*** *and it is not very moral*", FR82 "*vulnerable*", GE135 "*Unsafe and somewhat* ***inhuman****, it feels like I'm treated as just another customer for product XY*", GE139 "*exploited, unsafe,* ***like an object***".

Unfair practices: 8.6% of the participants focused on the methods practised by websites or companies that result in unfair or helpless situations such as expressed by UK1 "*there should be less third party tracking because sometimes* ***it is not you making a decision****, it is the adverts telling you to make a certain decision*", UK3 "*baddies, trying to* ***steal my info for their own illicit purposes***", UK8 "***betrayed*** *by the companies that sell my data*", UK25 "*... it feels a little* ***dishonest/sneaky***", GE46 "*surveilled and powerless. I have* ***no opportunity to disagree*** *to the tracking except not using the website...*", GE55 "***fucked because they can do whatever they want*** *and nobody stops them*", GE109 "*..****that I do not have privacy on the internet that I want*** *or that I am supposed to believe I have. I do not want companies to track my activities on the internet or sell my data but I need to agree to do so in order to use some services on the net*", or FR4 "*...Feel like we are* ***trapped***".

When participants went beyond expressing privacy/self invasion or unfair practices to name their emotional response to their dismay with TPT, we coded these under the specific emotion named, such as annoyance, anxiety, discomfort or distrust.

Annoyance: 12.5% participants named feeling tones traditionally categorised under anger-related emotions [73], such as annoyance, irritation, disgust or exasperation. These were expressed as emotional response to unfair practices, privacy invasion, lack of transparency, due to the presence of ads, or because something better should be offered. Example responses include: UK10 "***irritated****, unsecure, harassed,* ***annoyed, not happy*** *for them using my information without permission*", UK64 "***annoyed by it, that I'm being spied on***", GE50 "*Bothered, annoyed, stalked, disrespected*", GE44 "*Mostly I feel that third-party cookies are* ***annoying and not nearly transparent enough****, even if you're notified of them once you visit a website*", or GE20 "*that it tends to get annoying. once you search something out of curiosity your ads might be spammed with this very product that you in reality dont [sic] have the biggest interest in*".

Anxiety: 12.4% participants named feeling tones associated with anxiety, using words such as scary, worry, anxious, cautious, creepy or spooky. These were expressed as emotional response to the amount of information about someone that can be left online, the 'not knowing' about what TPT exactly is, how it happens, who accesses personal data and how to protect, and also when signs of tracking are noticed online. Example responses include: UK18 "*That it is a* ***pretty scary thing*** *seeing how much of yourself you leave on the Internet...*", UK41 "***Worried*** *that a third party that I don't know about is accessing my information*", UK53 "*It's pretty*

relevant in modern society with the increase in technology use, it's ***frightening*** *to not know enough about it to fully protect myself*", UK79 "*It would make me feel* ***cautious*** *about what information I am sharing online*", UK107 "*It sometimes* ***creeps me out*** *when I browse the internet for say make-up products and then the same webistes [sic] I visit appear in adverts on my Twitter feed...*", UK112 "*definitly [sic] makes me a bit nervous and a bit creepy almost like my phone is always listening to me*", or UK142 "*...it is a bit* ***spooky*** *to find links to things that you have been searching for and I do not like it at all*".

Discomfort: 9.1% participants reported feeling discomfort as a result of privacy loss or the lack of choice, not feeling at ease as they are not fully aware of the impact, and uncomfortable at the signs (by ads) that they are tracked. Participants used words such as uncomfortable, unsettled, overwhelmed, unpleasant, uneasy or disturbed. Example responses include: UK28 "***not comfortable****, i feel them to be intrusive. [sic] We don't have a choice, if we want to use a site ...*", GE23 "***Uneasy****, I don't want to have Facebook tracking me on pages other than their own*", UK67 "***unsettled by it*** *as I don't know who the third party is or what they are doing with my data*", and FR84 "*I feel* ***rather uncomfortable*** *when I come across ads that are clearly oriented towards content that I've already searched for on the web*".

Distrust: 3.9% participants expressed a lack of trust in websites or companies online, thereby expressing suspicion, wariness, or lack of trust. Example responses include: GE81 "*I feel it is a very* ***unknown and suspicious business****. Since you mostly agree via one click on a page long agreement that you haven't read carefully which results in unknow [sic] persons and institutions using your information*", FR32 "*I feel really suspicious, I do not rely on cookies and block them as possible as I can*", FR54 "***distrustful****, attentive, but non-paranoid*", and FR115 "*I am* ***wary about being tracked online****. I don't feel safe, I feel like I'm being exploited for my information*".

6.1.2 Sometimes Okay, Sometimes Not Okay

A group of participants were either sometimes okay and sometimes not-okay (ambivalent) or okay under certain conditions (okay_if) or okay because they were already protected (okay_protected). We visualise the differences between gender and country in Figure 3 and notice the following patterns: (1) more men than women expressed 'ambivalence' or combined 'ambivalence, okay_if, okay_protected' feelings in all countries; and (2) more UK participants expressed ambivalence compared to Germany and France, across both gender.

Ambivalent: 7.7% participants expressed that TPT can be both positive and negative. Example responses include: UK6 "***It can be okay sometimes but it's a bit bad that it can happen***", UK24 "*Pritty brutal [sic], but its the only way people make money on the web with ads anymore, with old*

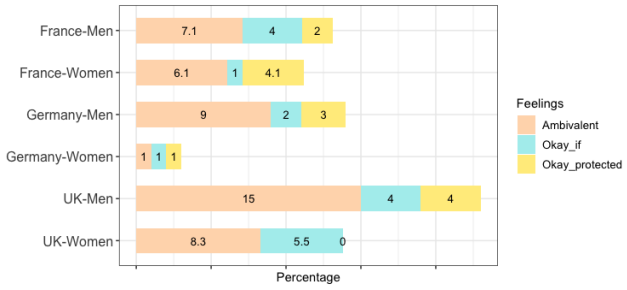

Figure 3: *ambivalent* or okay under certain conditions feelings (the x-axis shows % in each gender-country group with n=100 approx.)

people clicking the ads", UK58 "*A little intruded on but accept its a part of how the internet works*", GE26 "*exited [sic] at having an application that knows my desires better than i do, and a little scared at the exact same point*, and GE97 "*Ambivalent because it enables more free services, but can also be intrusive on privacy*".

Okay, if: Another 2.9% of participants expressed that they would be okay with TPT under certain conditions, such as personal data being used only to provide ads. Example responses include: UK13 "*...I don't mind seeing ads that are relevant to me and as long as the third party is not using the data in a harmful way then I don't mind*", GE35 "*Okay about collection of user data for advertising purposes as long as it is purely commercial and not political*", or UK23 "*It's ok as long as its not intrusive and no data is kept*".

Okay, protected: 2.3% participants expressed being okay with TPT because they took protective actions. Example responses include: FR177 "*I do not care because I use and adblocker [sic]*", GE64 "*relaxed because I block the most of it using DNS based blocking and adblockers*", and FR52 "*I use brave [sic] for this very reason but i know that sometimes you can access some website due to them blocking you if you don't accept the tracking*".

6.1.3 Okay or Indifference

A group of participants were okay with TPT, were indifferent, thought TPT was a necessity, or said that they felt nothing. We visualise the participant breakdown across gender and country in Figure 4 and notice that (1) slightly more women than men said that they had no feelings across all countries; and (2) more men were okay or indifferent, except for Germany.

Okay: 4.7% of participants said they were okay with TPT, in particular expressing that TPT was alright, or expressed positive feelings such as being content and comfortable with TPT, or focused on the advantages of TPT such as personalised ads, and a lack of concern. Example responses include: FR10 "*I understand that third party tracking is a part of what makes a lot of content on the internet free.* ***I feel ok with it***", UK2 "***I feel its alright i have no bad feelings towards***

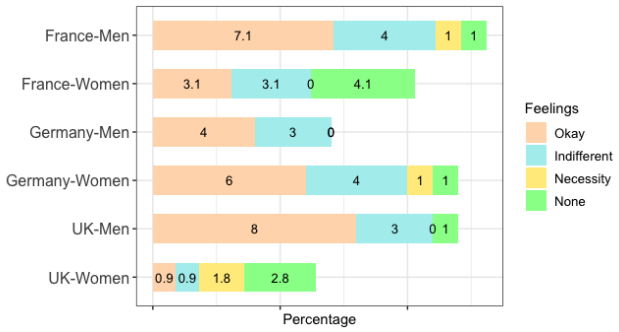

Figure 4: *okay or indifferent* feelings (the x-axis shows % in each gender-country group with n=100 approx.)

it", GE13 "***okay with it since it's only my online behavious that is being obersevd*** *[sic]. In addition most of the data collected is used for machine learning and not reviewed by actual humans*", UK5 "*I don't mind it*", FR88 "***comfortable**, I have no problem with that*", GE130 "*I sometimes like advertisments that* ***carter to my taste***", GE16 "***used too**, i think the web knows so much from me, i have nothing to hide, ok they can get this data too*", or GE93 "***not really concerned**, since those data might be valuable for marketing, but don't effect me personally in any way*".

Indifferent, necessity, none: 2.9% of participants said they were **indifferent** to TPT, such as by expressing indifference or not caring such as FR64 "*I feel a bit indifferent to be honest*", UK45 "*Not bothered*", GE90 "*Although it may be morally debatable, nobody really seems to care about it*", GE131 "*With regards to third-party tracking, I feel like i couldn't care less, honestly*". 0.7% participants spoke of the **necessity** of tracking online and of their acceptance of it, such as UK49 '*That it is just a necessary part of being online these days*", UK119 '*The amount of information out there is way too much to understand for a generic user. I accept that using the internet entails such addition to it*". 1.6% participants said that they felt nothing, such as UK65 '*Have no feelings*", GE124 '*no particular positive or negative emotion*", FR42 '*I don't feel any particular way about it*".

6.1.4 Other

Another group of responses did not point to emotional evaluation of TPT. Instead they called for regulation or said they were not aware of TPT. We grouped them under 'other'.

Call for Regulation: Although the GDPR makes provision for tracking protection, 2.9% of participants felt a need for (stronger) regulation, for completely banning TPT, or for particular legal coverage (such as opt-in only or more transparency). These responses show Internet users' un-awareness vis-à-vis the GDPR's coverage or their dis-satisfaction that the existing regulation do not do enough for privacy. Example responses included: FR43 "*I think it's a good idea but* ***it has to be regulated***", GE196 "*very dissatisfied.* ***Should be forbidden!*** *[sic]*", UK194 "*It* ***should be illegal**. I don't see how it can even be legal in the first place*, UK123 "*It is impossible to avoid as they cookies [sic] on the on every website which all communicate with each other this* ***should be banned***, GE103 "*Like it* ***should be opt-in only***", FR40 "*that it* ***should be made transparent*** *who can track us and for what reason, with an opt out*", and UK66 "*I think it is irresponsible and people* ***should be made aware very clearly*** *that they are being tracked, and can be damaging to people's mental health*".

Not aware: About 5.4% of participants said they were not aware of TPT or were confused by it, including UK48 '*No idea What this is [sic] I don't really take any interest in being safe on the Internet I mean I probably should but I don't*", or UK77 '*I don't know enough about this*".

6.2 Protective Actions Named by Participants

We investigate RQ2, that is "What tracking protective actions do individuals employ online?", given their gender and country differences. From the free-form text entered by participants (in responding to the questionnaire detailed in Section 4.2), we identified all mentions of PETs or other protection strategies.

We summarise the % participants naming each protective action, across gender and country in Figure 5. The noticeable patterns are that: (1) more women report to take no protective action (coded as 'none') in all countries; (2) more UK participants report to take no action compared to those from Germany and France, across both gender; and (3) the use of browser extension (coded as 'extension') is the most named action for men across all countries, whereas UK and German women prefer clearing/rejecting cookies (coded as 'clear_cookies').

34.7% responses were categorised as '**none**' as participants wrote 'none' or responded with text such as UK7 *"I'm not aware of how I can protect myself (I haven't knowingly allowed it)"*, or from GE48 *"nothing although i dont like Companys [sic] having so much data about me its really not that bothering to me so i just keep on using the internet as before"*.

65.3% of participants named at least one protection method. We list the type of protective method and provide example responses. For **extension to browser**: responses included FR93 *"I have installed Ublock Origin and added personalized precautions, and also Privacy Badger. Firefox also helps you with the cookies, fingerprint blocking,..."*. For **reject, limit or delete cookies**: UK144 responded *"None in particular other than declining the installation of cookies when they are mentioned."* or UK114 *"I always opt out of marketing requests and clear cookies"* or FR138 *"not much. I delete the cookies often, but that's it."* For **private browsing/browser**: FR61 responded *"Private browsing or onion routine (tor)"* and UK92 *"i use brave browser and ..."*. For **VPN (Virtual Private Net-**

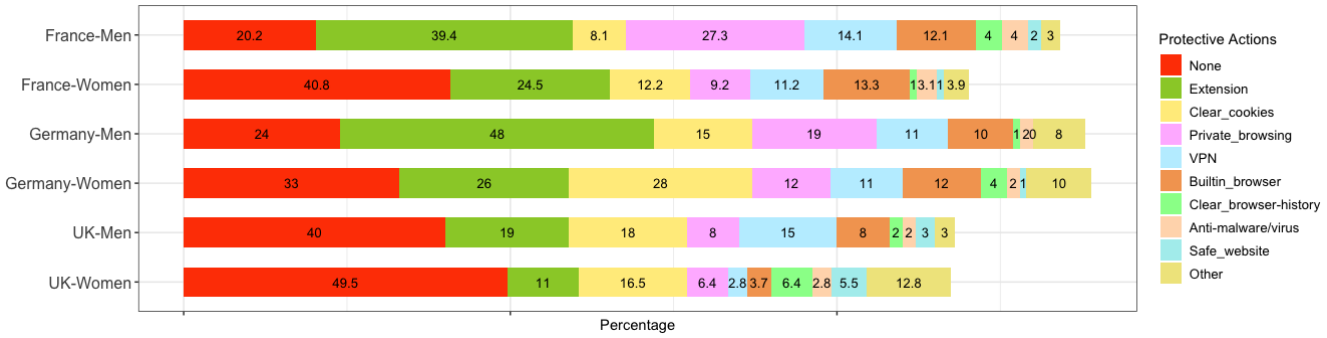

Figure 5: Reported *actions* across gender & countries (x-axis shows % in each gender-country group with n=100 approx.) *Note:* The first (red) portion of the bars refer to 'none', that is the % of participants not taking protective actions.

work): responses included FR92 *"I have a vpn, and when a website asks for my identity..."*. For **builtin browser options**: responses included GE78 *"My browser (firefox) blocks most third-party tracking scripts"*. We note that this protective method category refers to mainstream browser options rather than browsers built for privacy as in the 'private browsing/browser category'. For **anti -malware, -virus**: responses included UK3 *"antimalware in my antivirus software and also keeping everything updated [sic]"*. For **Clear browser history**: FR15 responded *"Every day I delete my browser history, all of it..."*. For **Safe website:** UK87 responded *"not visited web pages that have come up as suspicious"*.

Participants also mentioned strategies that we grouped under '**other**'. These included actions such as: *"I do not add my locations to social networking sites"* (UK79), *"I try to avoid public wifi unless absolutely necessary"* (FR148), *"avoid giving personal information, avoid social networks..."* (FR96) and *"I mostly use my work laptop and rely on it to have a good security software"* (GE174).

6.3 Association of Feelings with Protective Actions

We investigate RQ3, that is "How are individuals' feelings about third-party tracking associated with their protective actions?" We answer this RQ in two steps: first we provide an overall descriptive view of all the feeling tones together with the proportion of participants naming the different actions for each feeling tone, in Figure 6. Second we investigate the statistical association between feelings tones and protective actions via a multivariate analysis, producing a spatial map in Figure 7. We note that in contrast to the spatial map (in Figure 7) that plots the strength of association between feelings' action profiles and actions' feelings profiles, Figure 6 provides a descriptive view of the raw data.

Overall View: Figure 6 shows that for all expressed feeling tones, some participants responded to take no protective action, under 'none'. However, 'none' accounts for a high proportion of action types for feelings in the 'okay/indifferent' categories (while also noting the smaller number of participants naming these feelings).

Multivariate Analysis: We conduct a multivariate analysis of our dataset via a Correspondence Analysis (CA) [28], to investigate and visualise the relationship between expressed feelings and their protective action profiles. Our dataset is a contingency table of 16 rows (feelings expressed with regards to TPT) and 10 columns (protective actions named). In the following paragraphs, we report on the CA and results via the following steps (1) we compute the CA, (2) we visualise the spatial plot, and (3) we interpret the dimensions.

First, we compute the CA. We find a significant association between the row and column variables with $\chi^2 = 165.634$, $p = .037$, and the first dimension accounts for 44.58% of the variance in the data while the second dimension accounts for 17.36%. Together these two dimensions account for 61.94% of variability.

Second, we visualise the results via a spatial map, as provided in Figure 7. The spatial map shows the row and column profiles simultaneously in common space, where the proximity of the points demonstrates their similarity. For example, expressed feelings (blue points) that are closer together show more similar protective action profiles compared to those that are further apart.

Third, we interpret the dimension 1 (the x-axis, Dim1) in Figure 7 as it intuitively shows a spectrum of feeling tones, and note that we do not notice a pattern for dimension 2. Dim1 flows from the left with 'no feeling' (indifferent, none, not aware), to 'being okay/mild feelings' (okay, ambivalent, okay if, discomfort), to 'strong emotional response' with regards to TPT (not okay, annoyance, anxiety). The spatial map is intuitive in showing that the 'no feeling' end of Dim1 (negative end of x-axis) is more closely associated with no protective action (none in red) and furthest to protective actions (such as using clearing cookies, using an extension or builtin browser options). This corresponds to Figure 6 where the 'indifferent', 'none' and 'not aware' tones have highest proportions of no protective actions. In comparison, the 'mild feeling' section of Dim1 is closer to, and the 'strong emotional re-

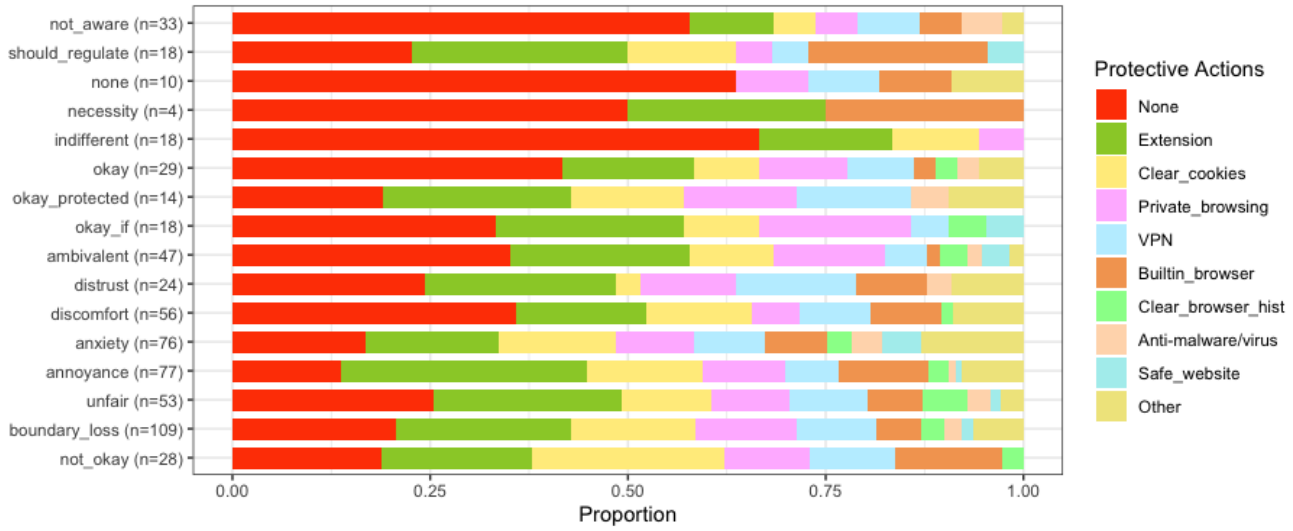

Figure 6: Overall view of feelings and actions, with x-axis showing the proportion of participants naming the different actions for each feeling tone. The y-axis shows feeling tones from *not_okay* to *distrust* that correspond to the *generally not okay/negative* category, tones from *ambivalence* to *okay_protected* corresponding to the *sometimes okay, sometimes not okay* category, tones from *okay* to *none* referring to the *generally okay/indifferent* category and *should_regulate* and *not_aware* for the *other* category.

sponse' end (positive end of x-axis) is most closely associated with, employing these protective actions. To summarise, (1) the feelings of being indifferent to TPT, having no feeling, being not aware of TPT, or viewing TPT as a necessity are furthest from action points; (2) feeling okay under certain conditions (okay, okay if, ambivalent) are nearer to action points; whereas (3) annoyance, anxiety emotional responses, as well as not okay, okay because one uses protection, call for regulation and feeling of boundary loss are nearest to protective action points.

6.4 How Feelings Predict Protective Actions

We investigate RQ4, that is "How do individuals' feelings about third-party tracking predict whether they take protective actions or not, given their gender and country differences?" We compute a mixed-effect binomial logistic regression with random intercept, with dependent variable 'taking protective action' versus 'not taking protective action' (as elicited from participant self-reports), and predictors gender, country and emotions. The model is constructed as follows: $action \sim (1|Participant) + Gender + Country + FeelingTones$. Feeling tones refer to the list of coded tones, except 'not_aware' which does not indicate any feeling. We test the model with all tones versus with only negative tones, and find that the model with only negative tones has a better quality than the one with all tones, as shown by its lower Akaike's Information Criteria (AIC) and Bayesian Information Criteria (BIC). We therefore present the model $action \sim (1|Participant) + Gender + Country + NegativeFeelingTones$. This model performs significantly better than an intercept-only baseline model with

Table 4: Binomial logistic regression for taking protective actions versus not.

	Est.	OR	95% CI	p-value
(Intercept)	-0.71	0.49	[0.32 - 0.75	.001***
men (vs women)	0.72	2.05	[1.43 - 2.95]	<.001***
Germany (vs UK)	0.60	1.83	[1.19 - 2.81]	.006**
France (vs UK)	0.58	1.78	[1.16 - 2.74]	.008**
not_okay: true (vs false)	1.19	3.28	[1.30 - 8.27]	.012*
boundary_loss: true (vs false)	0.93	2.53	[1.49 - 4.30]	.001***
unfair: true (vs false)	0.60	1.83	[0.95 - 3.50]	.070
annoyance: true (vs false)	1.35	3.84	[2.00 - 7.37]	<.001***
anxiety: true (vs false)	1.31	3.72	[1.98 - 6.99]	<.001***
discomfort: true (vs false)	0.41	1.50	[0.80 - 2.81]	.206
distrust: true (vs false)	0.73	2.08	[0.82 - 5.26]	.121

Note: Significance codes of '$***$'.001, '$**$'.01, '$*$'.05

$\chi^2(10) = 60.303, p < .001$. It has a good fit ($C = 0.701$), model accuracy of 70.6% and R^2 of 13%. Table 4 reports that men were twice more likely to take protective actions than women, with odds ratio (OR) $= 2.05, p < .001$, that German and French participants were approximately twice more likely to take protective actions than UK participants, with $OR = 1.83, p = .006$ and $OR = 1.78, p = .008$ respectively. In addition, participants who reported feeling tones of 'not_okay', 'boundary_loss' (invaded), annoyance or anxiety, also showed higher likelihood of taking protective actions (between $OR = 2.53$ and $OR = 3.84$), compared to those not naming these feelings.

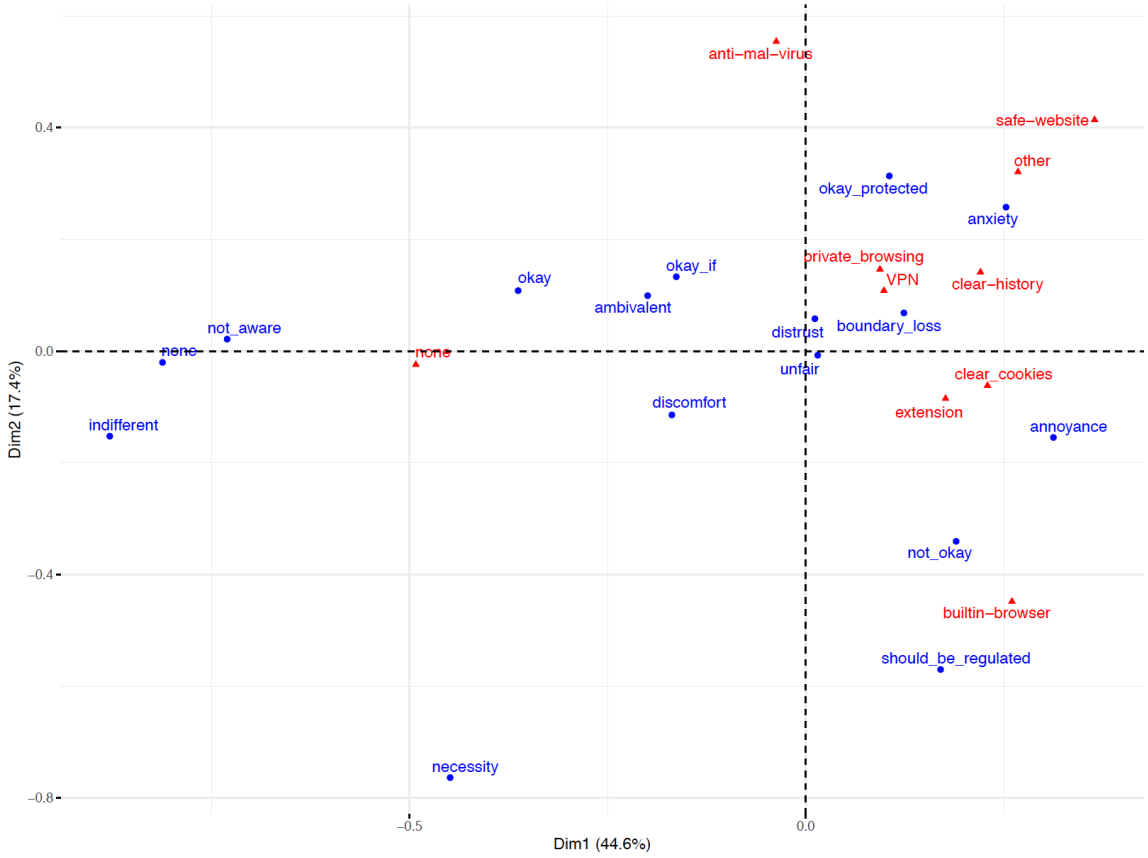

Figure 7: Spatial Map of Association between Feelings *(in blue)* and Protective Actions *(in red)*

7 Discussion

This paper makes a mixed-methods contribution (qualitative and quantitative) to user-centred privacy research, in particular on tracking protection. The main take-aways of this paper are that: (1) the majority of individuals (71.8%) have a negative feeling about tracking, (2) overall 34.7% do not take a protective action, some of whom also feel negatively, (3) protective actions are closely associated with (and predicted by) particular negative feelings, gender and country, and (4) there are indications of a gender gap and country differences in feelings and protective actions. In this section, we first discuss our findings in relation to literature and related work. Second, we discuss the implications for different stakeholders and offer recommendations and paths for future work.

7.1 Our findings in the wider research context

Feelings: While previous research did not find a clear causal link between individuals' cognitive evaluation of tracking (that is their understanding and mental models) and their protective behaviour [42], our findings support positions that feelings can provide useful inputs to judgments, decisions and behaviour when individuals' cognitive evaluation about a situation or event is in-accurate or incomplete [22]. This study therefore improves on cognitive-oriented investigations of tracking and user privacy.

Our participants' negative feelings include strong language and are spread across nuances of feeling tones, and in particular not only cover a perception of privacy threats, such as being monitored, of unfair practices and emotional responses of anger, anxiety, distrust or discomfort, but also the experience of a deep invasion to their personal realm. These findings augment previous findings of users' perception of privacy-invasiveness of tracking [44, 70, 71]. We also complement previous research [5, 44, 71], with some of our participants expressing other feelings, such as sometimes being okay with tracking, being okay under certain conditions, or being overall okay.

Protective Actions: In the context of the type of actions following particular negative feelings [38], we notice some slight differences in protective behaviour, albeit without clear distinctions, between annoyance and anxiety (Figure 6). However, we note the significant prediction of actively taking protective actions, by annoyance, anxiety or feeling invaded, compared to feeling discomfort, distrust or unfairness. In ad-

dition, while previous research reported individuals desisting from using services, such as location-based services, or taking retributive actions, such as issuing complaints, following anger and anxiety [31], our study is limited in not capturing these behaviours. However, of the 34.7% of participants reporting to take no protective action, the ones feeling negatively about tracking may be adopting passive coping methods such as acceptance or avoidance, as previously noted in relation to privacy threats [13, 31, 47].

Gender influence: Our findings provide indications of a 'privacy gender gap', complementing previous research on gender differences on concerns [7, 61, 79], where women in our study expressed more negative feeling tones combined, compared to men, who expressed more ambivalence or 'okay under certain condition' tones compared to women – yet men are twice more likely to take any protective actions, aligning with previous findings on protective behaviour [55, 61]. This suggests support for three decades old feminist critiques of the unequal nature of privacy online – that privacy is not equally on the side of women as it is for men [2, 41]. More research is needed into how these differences play out online and how to empower women to exercise their desired type and level of privacy.

National influence: We find that the British are less active in protective actions against tracking, and provided less reports of negative feelings, where action differences aligns to previous work [19]. Protective actions may relate to the effects of tracking being less clear or being less equipped to act compared to other modalities in the advertising ecosystem, where for example, a higher % of UK participants reported to object to direct marketing (i.e. being contacted directly via email or text messages) in the 2019 Eurobarometer survey, compared to those from Germany or France [17]. The British may also be less expressive or possibly have higher trust in authority mandated privacy protection. This phenomenon, with the national culture as an underlying cause, needs further investigation. Additionally, the impact of the depth of experience of privacy violation (as expressed by German and French's stronger language for boundary loss) on protective actions would benefit investigation.

7.2 Implications & Recommendations

We discuss the implications for different stakeholders, provide recommendations and highlight avenues for future work.

Users: Individuals' negative emotions, feelings of unfairness and deep invasion depict the dis-empowered reality of users, where protective action are also not necessarily effective. We recommend users to consider privacy-oriented browsers (such as the Brave browser, as chosen by some of our participants) over other options. In addition, to facilitate the development of more privacy-empowered online communities, specially supporting certain user groups, users may also be encouraged to openly share about their experiences of privacy issues and protection methods online, so as to facilitate the support of social and trusting connections on the feelings/experience–protective actions link.

Educators, privacy technology designers & providers: to understand who are more receptive (given their feelings) to privacy technologies, and to customise ways to up-skill individuals given their characteristics of gender and country. Other ways to improve privacy practice include free online courses, from reliable sources such as the national data protection authorities. We recommend that educators and privacy-enhancing technology (PET) designers make it clear what protection is offered by particular PETs, in a language that address users' concerns as expressed via their feelings about tracking, irrespective of their mental models. It would also be helpful to establish PETs repositories, and make vetted recommendations more accessible to the lay user. Existing lists for the general public include that of the Electronic Frontier Foundation's [24] or the European Agency for Cyber Security's (ENISA) [26].

Researchers: to deepen knowledge into the factors between particular negative feeling and protective action, such as awareness of and the obstacles to using protective methods and the support needed, across gender and country characteristic, or whether particular feeling-tones activate or inhibit actions. This includes research into different coping behaviours. In addition, individuals likely cope with tracking threats based on the combined judgement of cognition and affect, while influenced by factors such as perceived self-efficacy and response-efficacy – future work to include these variables, as well as awareness of the limitations of protection methods, where favoured tracking protection methods such as browser extensions, may not effectively block ads and trackers [53]. We also recommend research into diverse gender identities and user groups, in particular to understand their privacy experiences, vulnerabilities and challenges, and in comparison to the already available literature focused on cisgender. Furthermore, tracking issues also exist in platforms such as apps and IoT devices, and across platforms. While some efforts have been made for example in Apple's recent App Tracking Transparency (ATT) policy [4], it comes with its own issues such as increasing the number of privacy prompts and its effectiveness in improving user privacy remains as research questions.

Regulators and national data protection authorities: to set guidelines for actual fair practices, such as to avoid dark patterns that nudge users' acceptance despite their feelings and concerns, and for companies and service providers to demonstrate these fair attributes to customers, and to provide fair and inclusive practices for diverse user groups. It would also be helpful for researchers and designers to work with regulators and authorities, in preparing user-centric guidelines that support the deployment of new privacy technologies.

8 Conclusion

This paper adds to literature with an understanding of individuals' experiences of tracking and protection practices online. It adds to the mostly cognitive-focused literature of user privacy by providing novel findings on how feelings associates with and predicts protective actions. It describes a mixed methods approach, including (1) elicitation and synthesis of individuals' feelings and their own description of their protective actions, and (2) quantitative analyses and visualisation of associations. It discusses the findings in the context of previous work and what the findings mean for various privacy stakeholders and make recommendations. As highlight for future work, it proposes that although particular feelings about tracking are closely linked to protective actions, further research is needed into connecting these feelings with effective action, while gender/country differences point to needing customised methods and support for accessible protection.

Acknowledgements

This research was supported by a Newcastle University research fellowship. We would like to thank our shepherd, Simone Fischer-Hubner, and the Usenix Security 2022 reviewers for their feedback which helped to improve the paper.

References

[1] Lalit Agarwal, Nisheeth Shrivastava, Sharad Jaiswal, and Saurabh Panjwani. Do not embarrass: re-examining user concerns for online tracking and advertising. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, pages 1–13, 2013.

[2] Anita L Allen. *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield, 1988.

[3] American Psychological Association (APA). APA Dictionary of Psychology, 2021.

[4] Apple Developer. App tracking transparency, 2021.

[5] Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. Americans and privacy: Concerned, confused and feeling lack of control over their personal information. *Pew Research Center: Internet, Science & Tech (blog). November*, 15:2019, 2019.

[6] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The menlo report. *IEEE Security & Privacy*, 10(2):71–75, 2012.

[7] Lemi Baruh, Ekin Secinti, and Zeynep Cemalcilar. Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, 67(1):26–53, 2017.

[8] Antoine Bechara, Hanna Damasio, Daniel Tranel, and Antonio R Damasio. Deciding advantageously before knowing the advantageous strategy. *Science*, 275(5304):1293–1295, 1997.

[9] Grant Blank, Gillian Bolsover, and Elizabeth Dubois. A new privacy paradox: Young people and privacy on social network sites. In *Prepared for the Annual Meeting of the American Sociological Association*, volume 17, 2014.

[10] Grant Blank, William H Dutton, and Julia Lefkowitz. Perceived threats to privacy online: The internet in britain, the oxford internet survey, 2019. 2019.

[11] Moritz Büchi, Natascha Just, and Michael Latzer. Caring is not enough: the importance of internet skills for online privacy protection. *Information, Communication & Society*, 20(8):1261–1278, 2017.

[12] Farah Chanchary and Sonia Chiasson. User perceptions of sharing, advertising, and tracking. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*, pages 53–67, 2015.

[13] Hichang Cho, Pengxiang Li, and Zhang Hao Goh. Privacy risks, emotions, and social media: A coping model of online privacy. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 27(6):1–28, 2020.

[14] Hichang Cho, Milagros Rivera-Sánchez, and Sun Sun Lim. A multinational study on online privacy: global concerns and local responses. *New media & society*, 11(3):395–416, 2009.

[15] Gerald L Clore, Karen Gasper, and Erika Garvin. Affect as information. *Handbook of affect and social cognition*, pages 121–144, 2001.

[16] European Commission. Data protection - special eurobarometer 431. *Special Eurobarometer*, 2015.

[17] European Commission. The general data protection regulation - special eurobarometer 487a. *Special Eurobarometer*, 2019.

[18] European Commission. eprivacy regulation: Shaping europe's digital future, 2021.

[19] Kovila PL Coopamootoo. Usage patterns of privacy-enhancing technologies. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pages 1371–1390, 2020.

[20] Kovila PL Coopamootoo and Thomas Groß. Why privacy is all but forgotten - an empirical study of privacy and sharing attitude. *Proceedings on Privacy Enhancing Technologies*, 4:39–60, 2017.

[21] Dan Cvrcek, Marek Kumpost, Vashek Matyas, and George Danezis. A study on the value of location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 109–118, 2006.

[22] Antonio Damasio. *Descartes' error: Emotion, reason and the human brain*. Random House, 2008.

[23] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. In *Network and Distributed System Security Symposium*, 2018.

[24] Electronic Frontier Foundation. Tools from EFF's Tech Team, 2021.

[25] Steven Englehardt and Arvind Narayanan. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pages 1388–1401, 2016.

[26] European Agency for Cyber Security. Online privacy tools for the general public, 2021.

[27] Fariborz Farahmand and Firoozeh Farahmand. Privacy decision making: The brain approach. *Computer*, 52(4):50–58, 2019.

[28] Michael Greenacre. *Correspondence analysis in practice*. Chapman and Hall/CRC, 2017.

[29] Geert Hofstede. *Culture's consequences: International differences in work-related values*, volume 5. sage, 1984.

[30] Jennifer L Hughes, Abigail A Camden, and Tenzin Yangchen. Rethinking and updating demographic questions: Guidance to improve descriptions of research samples. *Psi Chi Journal of Psychological Research*, 21(3):138–151, 2016.

[31] Yoonhyuk Jung and Jonghwa Park. An investigation of relationships among privacy concerns, affective responses, and coping behaviors in location-based services. *International Journal of Information Management*, 43:15–24, 2018.

[32] Flavius Kehr, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6):607–635, 2015.

[33] Agnieszka Kitkowska, Mark Warner, Yefim Shulman, Erik Wästlund, and Leonardo A Martucci. Enhancing privacy through the visual design of privacy notices: Exploring the interplay of curiosity, control and affect. *decision-making*, 1(4):21, 2020.

[34] Bart P Knijnenburg and Alfred Kobsa. Making decisions about privacy: information disclosure in context-aware recommender systems. *ACM Transactions on Interactive Intelligent Systems (TiiS)*, 3(3):1–23, 2013.

[35] Hanna Krasnova and Natasha F Veltri. Privacy calculus on social networking sites: Explorative evidence from germany and usa. In *2010 43rd Hawaii international conference on system sciences*, pages 1–10. IEEE, 2010.

[36] Richard S Lazarus and Susan Folkman. *Stress, appraisal, and coping*. Springer publishing company, 1984.

[37] Pedro Giovanni Leon, Ashwini Rao, Florian Schaub, Abigail Marsh, Lorrie Faith Cranor, and Norman Sadeh. Privacy and behavioral advertising: Towards meeting users' preferences. In *Proceedings of the Symposium on Usable Privacy and Security*, 2015.

[38] Jennifer S Lerner and Dacher Keltner. Fear, anger, and risk. *Journal of personality and social psychology*, 81(1):146, 2001.

[39] Han Li, Rathindra Sarathy, and Heng Xu. The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, 51(3):434–445, 2011.

[40] George F Loewenstein, Elke U Weber, Christopher K Hsee, and Ned Welch. Risk as feelings. *Psychological bulletin*, 127(2):267, 2001.

[41] Catharine A MacKinnon. *Toward a feminist theory of the state*. Harvard University Press, 1989.

[42] Arunesh Mathur, Jessica Vitak, Arvind Narayanan, and Marshini Chetty. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018)*, pages 103–116, 2018.

[43] Jonathan R Mayer and John C Mitchell. Third-party web tracking: Policy and technology. In *2012 IEEE Symposium on Security and Privacy*, pages 413–427. IEEE, 2012.

[44] Aleecia McDonald and Lorrie Faith Cranor. Beliefs and behaviors: Internet users' understanding of behavioral advertising. Tprc, 2010.

[45] William Melicher, Mahmood Sharif, Joshua Tan, Lujo Bauer, Mihai Christodorescu, and Pedro Giovanni Leon. (do not) track me sometimes: Users' contextual preferences for web tracking. *Proceedings on Privacy Enhancing Technologies*, 2016(2):135–154, 2016.

[46] Isabelle Oomen and Ronald Leenes. Privacy risk perceptions and privacy protection strategies. In *Policies and research in identity management*, pages 121–138. Springer, 2008.

[47] Jonghwa Park, Hanbyul Choi, and Yoonhyuk Jung. Users' cognitive and affective response to the risk to privacy from a smart speaker. *International Journal of Human–Computer Interaction*, pages 1–13, 2020.

[48] Yong Jin Park. Do men and women differ in privacy? gendered privacy and (in) equality in the internet. *Computers in Human Behavior*, 50:252–258, 2015.

[49] UK Parliament. Data protection act 2018. *URL https://services. parliament. uk/bills/2017-19/dataprotection. html*, 2018.

[50] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70:153–163, 2017.

[51] James Pierce, Sarah Fox, Nick Merrill, and Richmond Wong. Differential vulnerabilities and a diversity of tactics: What toolkits teach us about cybersecurity. *Proc. ACM Hum.-Comput. Interact.*, 2(CSCW), November 2018.

[52] Gaston Pugliese, Christian Riess, Freya Gassmann, and Zinaida Benenson. Long-term observation on browser fingerprinting: Users' trackability and perspective. *Proceedings on Privacy Enhancing Technologies*, 2020(2):558–577, 2020.

[53] Enric Pujol, Oliver Hohlfeld, and Anja Feldmann. Annoyed users: Ads and ad-block usage in the wild. In *Proceedings of the 2015 Internet Measurement Conference*, pages 93–106, 2015.

[54] Ashwini Rao, Florian Schaub, and Norman Sadeh. What do they know about me? contents and concerns of online behavioral profiles. *arXiv preprint arXiv:1506.01675*, 2015.

[55] Elissa Redmiles. Net benefits: Digital inequities in social capital, privacy preservation, and digital parenting practices of us social media users. In *Proceedings of the International AAAI Conference on Web and Social Media*, volume 12, 2018.

[56] Elissa M Redmiles, Ziyun Zhu, Sean Kross, Dhruv Kuchhal, Tudor Dumitras, and Michelle L Mazurek. Asking for a friend: Evaluating response biases in security user studies. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1238–1255, 2018.

[57] Philip J Reed, Emma S Spiro, and Carter T Butts. Thumbs up for privacy?: Differences in online self-disclosure behavior across national cultures. *Social science research*, 59:155–170, 2016.

[58] Mark Rowan and Josh Dehlinger. Observed gender differences in privacy concerns and behaviors of mobile device end users. *Procedia Computer Science*, 37:340–347, 2014.

[59] Florian Schaub, Aditya Marella, Pranshu Kalvani, Blase Ur, Chao Pan, Emily Forney, and Lorrie Faith Cranor. Watching them watching me: Browser extensions impact on user privacy awareness and concern. In *NDSS workshop on usable security*, pages 1–10, 2016.

[60] Ann E Schlosser, Sharon Shavitt, and Alaina Kanfer. Survey of internet users' attitudes toward internet advertising. *Journal of interactive marketing*, 13(3):34–54, 1999.

[61] Kim Bartel Sheehan. An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, 13(4):24–38, 1999.

[62] Fatemeh Shirazi and Melanie Volkamer. What deters jane from preventing identification and tracking on the web? In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pages 107–116, 2014.

[63] Paul Slovic, Melissa Finucane, Ellen Peters, and Donald G MacGregor. Rational actors or rational fools: Implications of the affect heuristic for behavioral economics. *The Journal of Socio-Economics*, 31(4):329–342, 2002.

[64] Tal Soffer and Anat Cohen. Privacy perception of adolescents in a digital world. *Bulletin of Science, Technology & Society*, 34(5-6):145–158, 2014.

[65] Luke Stark. The emotional context of information privacy. *The Information Society*, 32(1):14–27, 2016.

[66] Statista. Number of internet users in european countries as of june 2019, 2019.

[67] The European Parliament and the Council of the EU. Regulation (EU) 2016/679 of the European Parliament and of the Council, April 2016.

[68] Wiebke Thode, Joachim Griesbaum, and Thomas Mandl. " i would have never allowed it": User perception of third-party tracking and implications for display advertising. In *ISI*, pages 445–456, 2015.

[69] Robert Thomson, Masaki Yuki, and Naoya Ito. A socio-ecological approach to national differences in online privacy concern: The role of relational mobility and trust. *Computers in Human Behavior*, 51:285–292, 2015.

[70] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. Americans reject tailored advertising and three activities that enable it. *Available at SSRN 1478214*, 2009.

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

[72] Yang Wang, Huichuan Xia, and Yun Huang. Examining american and chinese internet users' contextual privacy preferences of behavioral advertising. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*, pages 539–552, 2016.

[73] David Watson and Lee Anna Clark. The panas-x: Manual for the positive and negative affect schedule-expanded form. 1999.

[74] Rainer Westermann, Kordelia Spies, Günter Stahl, and Friedrich W Hesse. Relative effectiveness and validity of mood induction procedures: A meta-analysis. *European Journal of social psychology*, 26(4):557–580, 1996.

[75] Alan Westin. Privacy and american business study. *Retrieved online November*, 1:2010, 1997.

[76] Kim Witte. Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, 59(4):329–349, 1992.

[77] Donghee Yvette Wohn, Jacob Solomon, Dan Sarkar, and Kami E Vaniea. Factors related to privacy concerns and protection behaviors regarding behavioral advertising. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems*, pages 1965–1970, 2015.

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

[79] Seounmi Youn. Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer affairs*, 43(3):389–418, 2009.

A Codebook

Table 5: Codebook of Feelings with regards to Third-Party Tracking (with example words mentioned in responses)

Emotion	Explanation & Example words in responses
Not Okay	Participants say 'not okay', 'not like'
Boundary loss	There is a sense of loss of boundaries wrt to info privacy, or beyond info boundaries E.g words: invasion of privacy, tracked,unsafe, naked, raped, exposed, invaded, watched, violated, exploited, insecure
Unfair practice	A sense of unfair actions from others E.g. words: used, misused, sold, manipulated, ill-informed, not you making decisions, no chance to decide, info stolen, betrayed, dishonest, sneaky, sleazy, immoral, illegal, like a rat-test subject. No control, trapped, cheated, obscure, powerless, unethical
Annoyance	Expressed anger-related emotion E.g. words: Annoyed, angry, disgust, irritated, exasperated, bothered
Anxiety	Expressed worry-related emotion E.g. words: Scared, worry, cautious, creepy, spooky, unnerving, concern
Distrust	Expressed suspiciousness E.g. words: Suspicious, not trust, wary, uncertain
Discomfort	Expressed discomfort or overwhelm E.g. words: uncomfortable, overwhelm, unsettled, unpleasant, uneasy, disturbed
Should be regulated	Expressed that third-party tracking should be regulated/protected E.g. words: should be regulated, should be protected, should be banned, should be made aware, should be transparent
Okay	Expressed that they were overall okay with tracking or used specific words. E.g. words: I am okay, I am alright
Ambivalent	Expressed that they are sometimes okay sometimes not okay, fine for this reason but not fine of other reason
Okay, protected	Expressed that they were okay with tracking because they protect themselves anyway. E.g. words: I am okay as/because I protect myself.
Okay, if	Expressed that they would be okay with tracking IF .... E.g. words: I am okay if they do that / ... if I know / ... but have to inform
Necessity	E.g. words: it's a necessity/a must, impossible for normal user to do
Not aware	E.g. words: I don't know enough, I don't know
Indifferent	E.g. words: indifferent, insensitive, I don't care
None	Participants say that they feel nothing