Theory/Practice Transfer Paper 4

Matriculation number:	8240
Accepted topic:	Analysis of behavioral conditioning by privacy policy modals
Bachelor's programme, centuria:	Bachelor of Science — Angewandte Informatik, A17a

Contents

List of Figures

1 Introduction

The internet is an essential good in todays life. It simplifies communication on a global scale, makes information about almost anything easily accessible from virtually anywhere, allows shopping without ever leaving the comfort of home, eases the planning efforts of individuals and companies alike, and poses a great opportunity for researchers. Through all these ways it also allowed companies to easily scale to a global market and even opened up new business opportunities. However, back in the day of dial-up modems and Netscape regulations were nowhere to be seen and remained scarce for a long time. Over the years, local regulations like the Telemediengesetz in Germany developed in many countries around the world.

This posed a unique challenge for web content as it had to adhere to different regulations in different areas. It became hard to comply with all regulations in every area where the website was accessible. Companies were forced to heavily invest in research on compliance and new technologies to stay on top of it all. [1]

In 2018 the General Data Protection Regulation (GDPR) has taken effect in the European Union (EU) which created a paradigm shift [2]. Instead of giving users the option to opt-out of personal data collection, it enforces an explicit approval. Thus the focus of companies shifted from making users not notice the opt-out to potentially tricking them into opting-in to being tracked. However, one may not blame the companies for this behavior since their business case heavily relies on implicit feedback and tracking data from customers. It may even be considered a requirement to stay competitive and maintain a profitable online presence.

Looking at it from the perspective of users makes this a troublesome move. The decision on whether or not to allow such tracking is now in their hands. To cite the GDPR, users should give consent through "a clear affirmative act establishing a freely given, specific, informed and unambiguous indication [...]" [3]. While many companies are still struggling to comply with these requirements [1], it becomes more commonplace for consent questions to pop up upon visiting a website.

Since the relevant data is of high value for companies the question arises whether users are being manipulated and tricked into giving consent. This will be the research question for this paper. To answer it I will begin by researching potential manipulation methods using available literature. Then an attempt to prove the real-world applicability and use of such manipulation taking place will be made by conducting an interactive survey.

2 User conditioning on the web

To begin with the term of operant conditioning has to be defined. In 1937 B. F. Skinner published a research paper in “The Journal of General Psychology” coining the term. His theory is used to describe how behavior is influenced by the rewards and consequences following it. [4]

For this research paper, the scope will be limited to a more focused topic called negative reinforcement. It describes how the behavior of an operant can be influenced by introducing a negative stimulus. Skinner proposed and conducted an experiment in which he placed a rat into a cage. Then, a mild electric shock — the negative stimuli or reinforcer — was introduced. The box also contained a lever which deactivates the electricity. The rat in the experiment quickly learned to press the lever once the stimulus was introduced. Taking it one step further, a lamp was added which turned on just before the actual stimulus was activated and the operant quickly learned to press the button in response to the lamp to avoid the negative reinforcer. There is a more common version of this experiment in which food is released when the lever is pressed. This describes the opposite kind of conditioning and is called positive reinforcement. [5]

To explain why negative reinforcement might be affecting users on the web, a clearer picture of how websites are handling consent is required. Users have been exposed to privacy policies, cookie notices, and tracking consent mechanisms for a long time [6]. However, recently there has been a fundamental change. Up till now, websites were freely accessible and such mechanisms only occupied a limited portion of the screen. This changed with recent legislation, making it mandatory to collect consent before actually tracking the visitors. To get an insight into how this affected access to websites, a small analysis will be conducted.

First, a list of the top 300 domains has been retrieved from a large SEO contractor [7]. Since the web is changing every day, a snapshot of this list at the time of writing has been included in the accompanying GitHub repository[1]. Second, each of these websites has been visited from within Europe[2] and manually categorized as follows. There are categories and subcategories. Categories describe the type of consent mechanism in place (Modal, Banner, Other) and subcategories describe the subtype of mechanism. For banners and modals there are three types:

Info: The consent mechanism is only informing the user about the collection of data and does not present a choice. Some variations may ask the user to leave the page if they do not consent.

Config: An option to manually configure which data can be tracked is present, however, users can not reject all tracking with a single click.

Reject: Users are presented with a direct option to reject tracking. This subtype may also include a config option but it is possible to reject with a single click.

For the “Other” category there are three subcategories:

Nothing: No consent mechanism is present. This may not indicate that the page is not tracking the user regardless.

Blocked: The page is regionally blocked within Europe, preventing access in regions where the new legislation is in effect.

Invalid: There is no valid web-content behind the domain name. This has been the case for content

[1] Link excluded in this version of the document

[2] To rule out any potential regional variations in the websites

delivery networks, services, and others. It does not indicate that the domain has no content, just that there is no publicly visible content.

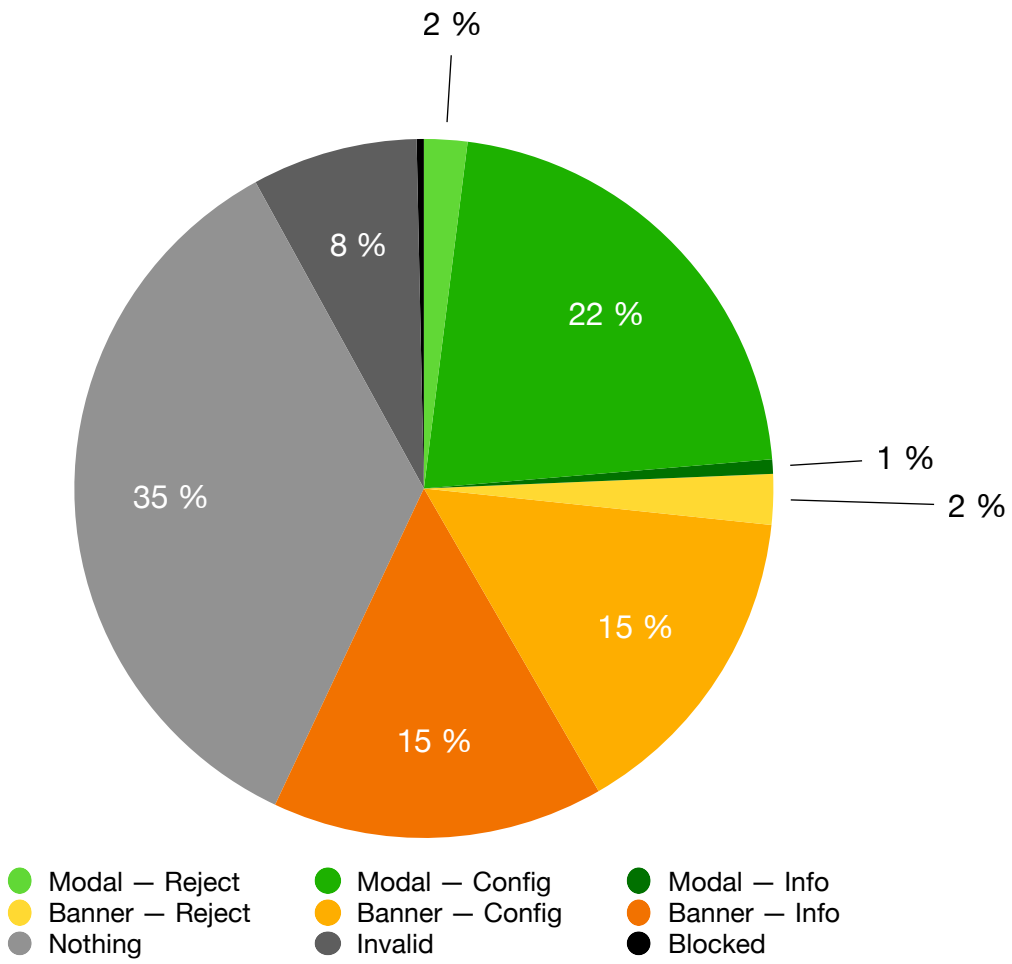

Figure 1: Tracking consent mechanisms of top 300 domains

The pie chart seen in figure 1 contains the previously mentioned categories and subcategories. The former are identified by the groups of colors (green, orange, grey) while the latter is represented by different shades of the aforementioned colors. Looking at the “Other” shard it becomes immediately obvious that over a third of all pages do not present any kind of consent mechanism or are regionally unavailable. Note that it has not been evaluated whether or not pages in this category are still tracking users. To answer this further research is required. Looking at the other two categories, banners do prevail with 32% over 25% of pages with modals. However, almost half of the banners do not ask for consent but instead only inform the users that tracking takes place. With modals, the story is slightly different. Two websites did solely inform the user while an overwhelming majority of modals are presenting a complex configuration menu which requires at least three clicks to reject tracking. Only six domains did provide a modal with a one-click method to do so.

Looking back at operant conditioning, a quarter of all websites have become obstructed by a consent

workflow out of which almost 90% makes it very complicated and time-consuming to visit the website without being tracked. In this instance, the consent flow can be seen as a negative stimulus that prevents the user from accessing the desired content. Research has revealed that humans are likely to prefer immediate stimuli that only last for a short time period and have shown impulsive behavior while influenced by a negative reinforcer [8]. This knowledge is being used by todays consent workflows which provide an easy, short route of evading the stimuli by agreeing to data collection while making it complicated and time-consuming to disallow tracking. Whether or not this is a deliberate act or a coincidence is unclear. However, websites could very well have designed modals in a way that favors disallowing and makes selectively agreeing to certain tracking providers the more complex option. This not being the case on every website observed makes a strong argument for it being a deliberate choice[3]. Overall, it seems very likely that users are being influenced through negative reinforcement by the new consent mechanisms. Old, banner-style consent mechanisms are less likely to have this effect since the stimulus is too weak and a majority of people are ignoring them altogether [6].

3 Survey

Now that you are familiar with conditioning and why it might apply in the context of the web, evidence is required that it applies in the real world. There are two factors we will look at in this paper. The first one focuses on whether or not users do consider the content of privacy-related modals or act based on assumptions and prior knowledge. The second aspect is whether or not users are consistently choosing one strategy to deal with such modals. If some users (which ideally consider themselves privacy-aware) always reject the policies while others always accept it, it could indicate a strategy based on a real preference. However, if users vary frequently between strategies and for example abandon the rejection of a policy, if the process is too complicated, it would indicate that decisions are not solely based on the users' preference.

As this is a topic that heavily relies on the users' psychology, a plain interview is out of the question. While it is likely possible to design an interview so it would yield reasonable results, there are easier methods available. As user preference plays a big role a sufficient number of participants is required. This makes an interactive survey an attractive choice as it can be scaled effortlessly. To answer the initial questions data has to be collected during the survey and a few factors listed below have to be controlled:

User interaction: To determine whether or not the user follows a consistent strategy the path he takes through the modals on various websites has to be observed. This can be realized by either tracking all JavaScript events fired within the browser or by recording the screen and visualizing touch/mouse interactions and reviewing it later.

Browser control: To consistently display websites to all participants and make sure the same privacy policy modals show up, some degree of control has to be exerted over either the websites or the browser[4].

Page control: Verifying whether or not users consider the content of privacy modals requires modifications to such modals — more on that in the design phase. This requires writing access to a website's

[3] Further research is required to definitively prove this

[4] Note that some websites share the same service provider for modals and answering a modal on one page might hide it on another one (NextRoll, Inc. is an example for one such provider)!

source code or access to the browser to display a fake website[5].

The above criteria leave a couple of options with varying complexity. The conceptually simplest would be to modify an existing website that has live traffic. However, this option requires access to such a page and legal constraints make this unviable. Another option would be to implement a proxy server that filters and modifies traffic to create a sculpted scenario as required for this survey. Again, this requires consent from the users, modifications to the operating system of the participants, and therefore scaling is hard to achieve. The widespread adoption of traffic encryption further complicates this option. That leaves one more option of running the survey on a device that has been prepared and configured specifically for this survey. Screen recording and visualization of user interactions can be achieved easily, controlling the browser is possible and depending on the operating system it is viable to trick the browser into displaying a fake website. However, this approach does not scale very well as it requires one-on-one interaction with each participant. To circumvent this issue, a purpose-built mobile application for tablets could be developed. It provides all the options available with the single-device approach and makes distribution and thus scaling easy. As an additional bonus, it reduces the number of health precautions required due to the current pandemic because human interaction is reduced.

3.1 Design

This subsection covers various design decisions made for both the app containing the survey as well as the survey workflow itself.

3.1.1 Application

Due to prior knowledge with iOS app development, availability of appropriate devices, and the availability of APIs that cover all requirements, the Apple iPad has been chosen as the survey platform. An interactive survey application has been developed. The ResearchKit framework has been employed to simplify the creation of a survey workflow. Browser automation and control has been implemented using the WebKit framework. Other UI components including a frontend for the browser have been implemented using the SwiftUI and UIKit system libraries. Screen recording has been implemented using the `RPScreenRecorder` class from ReplayKit and H.265 encoding of the resulting frames was done using the `AVAssetWriter` from AVFoundation. The data from both ResearchKit (participants answers to questions, duration of tasks) and AVFoundation (screen recordings) are being bundled as a tar ball using the SWCompression framework. This file will be sent to the authors through the Telegram app using a specialized UI component. The source code of this application together with all scripts used for evaluation is available on GitHub[6].

3.1.2 Workflow

The survey begins by introducing the authors and why this survey is being conducted. Then, the user is notified about the types of data being collected and that he can cancel at any time. Next, the participant

[5] As one can expect, this is considered a major security concern under real-life circumstances and thus not easy to achieve

[6] The link has been excluded from this version of the document to retain the anonymity of the author

is asked whether his data may be shared publicly. The data of all participants that agreed to this will be published in the previously mentioned GitHub repository. After that, the user is requested to start the screen recording using a system dialog. Now the user is introduced to the concept of assignments and how to solve them (rough explanation of the user interface). What follows is several tasks that require the participant to interact with various websites. These have been designed to distract from the actual focus of the survey and the answers to these are not being stored or validated. To prevent interference through factors like annoyance their order will be randomized for each participant. One task involves a website that has been rigged to include a bogus privacy policy text that makes the user sell his kidney. While not legally valid, this makes it easy to check later if the user noticed this fake policy. There are six assignments as previous surveys have shown that a higher number makes the overall survey too long. The goal is for the survey to take roughly eight minutes. Once all assignments have been completed the user is asked a few questions:

- Data privacy
  - How important is data privacy to you on a scale from 1 to 10?
  - Does the GDPR improve the privacy of your data?
  - Do you usually try to get rid of modals or configure them according to your preference?
  - Did you notice that you sold your left kidney?
- Demography
  - What describes your occupation best? [School, University, Work, Pensioned]
  - Are you working in the computer science sector?
  - How good are your computer skills on a scale from 1 to 10?

Finally, the user is given the option to share his contact information to be notified about the results.

3.1.3 Websites & Assignments

Regarding websites, five german pages with modal privacy policy popups have been chosen at random. These include Heise (https://heise.de), UCI (https://uci-kinowelt.de), Postillon (http://der-postillon.com), famila (http://famila.de) and ING-DiBa (https://ing.de). To forge a modal, a small British web-shop selling wooden ducks called Dcuk (https://dcuk.com) has been selected — the forged modal can be seen in figure 2. The assignments and consent mechanism designs are listed below, screen captures of each page can be found in the Appendix (section A.2).

Heise: This page contains a large, colored accept button and a transparent but outlined configure button side by side. The latter leads to a rather simple configuration menu with only a few switches. However, it theoretically requires only two clicks to reject the policy. The assignment on this page is to find the duration of the trial for their premium news subscription service called “Heise+”.

UCI: As opposed to Heise, the consent modal contains three buttons. The first one accepts the policy, the second rejects it, and the third opens a complex configuration menu. They are vertically stacked and have decreasing highlights with the first one having a prominent background color, the second one is just text, and the third one is small text. Participants have to find the monthly price of the cinema subscription called “UCI Unlimited”.

Postillon: The modal of this page is larger than the other two and contains a filled accept button and an outlined configure button. The configuration menu is rather complex with multiple tabs and hundreds of switches. Rejecting the policy technically takes two clicks, however, users might be tricked into pressing an “Accept All” button in the bottom right of the config interface. To fulfill the assignment,

the name of the author of the first edition has to be found.

famila: Of all pages, this is probably the most straightforward. The modal contains three checkboxes for different tracking sources, a accept all button, and a button to save the selected ones where the default is to reject all non-necessary cookies. The reject/save button is grey while the accept button is green and they are vertically stacked. Users have to find the name of the head of operations at their closest store.

ING-DiBa: This page contains a modal that has a filled orange accept button in the bottom right and a text-based config button in the bottom left. The settings are rather straightforward and it requires two clicks to reject the policy. The assignment on this page involves finding the minimum monthly salary required for the personal bank account to be free.

Dcuk: The consent mechanism of this page has been forged to look authentic. The website is loaded by the bookmark is not the remote page but instead a local HTML file containing an iframe. Once the content of the frame has finished loading, a forged overlay will be shown by local JavaScript. It can be seen in figure 2 and the source code is available in the previously mentioned GitHub repository. To complete the task, the user has to find the price of a so-called “Graduation Dinky Duck”.

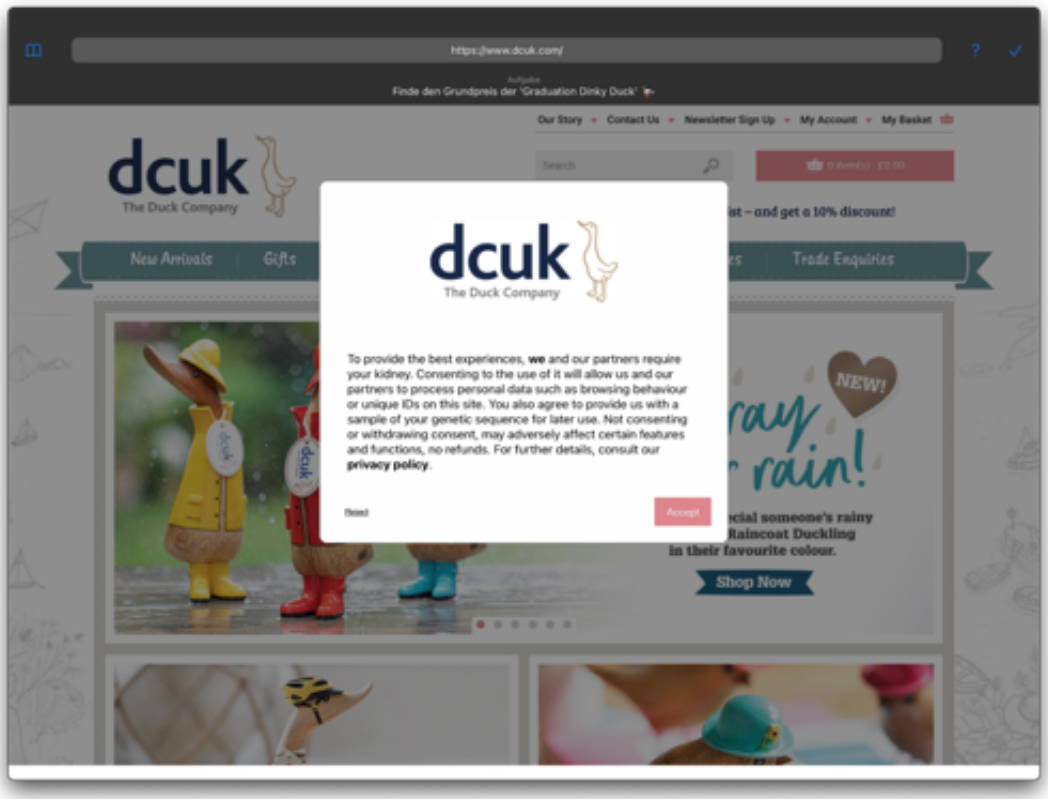

Figure 2: Website — Dcuk Shop with forged modal

3.2 Distribution

Now that a survey has been determined as the method of choice, it is going to be implemented and distributed. As it is an iPadOS app there are limited distribution options available. Publishing it to

the App Store publicly is not viable since it does not align with some of the stores' review guidelines and contains personal contact information of the authors. An alternative is the TestFlight service. It provides a way to distribute an app to up to 10.000 beta testers using just a link. This link can then be distributed to personal contacts which in turn distribute it to their peers with appropriate devices. People that have the application installed on their device can in turn have other acquaintances go through the survey. As there are no other simpler solutions available[7] and since this approach is rather straightforward it will be used. Throughout two weeks data will be collected with a goal of equal to or greater than 20 participants. Past surveys have shown this number to be a reasonable expectation for the collection period and while it does not produce representative results it suffices to provide a rough idea of what representative results may look like[8].

4 Findings

The survey has been conducted over a period of 15 days and a total of 26 results have been collected. Out of those, one participant's result was unusable due to file corruption during the screen recording. A total of 19 participants gave consent to share their results with the public and the corresponding data can be found in the accompanying GitHub repository[9].

4.1 Overall

Even though the overall results may not give direct insights into the conditioning status of participants, it may still contain valuable insights. The average duration of the survey was just over eight minutes, closely matching the original goal. Regarding the GDPR 42% (11) of the participants would consider it an improvement to data privacy while 58% state that it did not make any significant impact. Out of all privacy policies shown, 59% (89) have been accepted and 41% (61) rejected. However, the ratio varies heavily between pages with famila and the UCI clocking in at 32% and 48% of accepted policies respectively while pages like Heise and ING-DiBa are closer to 75% as can be seen in figure 7. While it is not the goal of this paper to determine differences in design and workflow that influence user behavior, it can be assumed that the simpler rejection path of the former — requiring only a single click — caused these numbers while the more complex workflows and hidden rejection methods on the latter pages eventually forced users into accepting policies. Video recordings also showed some participants attempting to reject policies but were then either tricked into accepting them by presenting an "Accept All" button at the end of the configuration page or having a complex workflow that led to the user backtracking and using the simpler accept workflow. Some users also exhibited patterns of annoyance especially on pages that repeatedly showed the popup after navigation when the cookies were rejected, ultimately accepting the policy.

[7] At least with the limited research done
[8] Which, given the scope of both length and time of this research paper, is acceptable
[9] Link excluded in this version of the document

4.2 Demographics

The group demographics split into sixteen students and nine persons working full-time. No retired persons or children did participate. The same distribution can be seen in persons working in the software development sector with sixteen doing so and nine working in other areas. Unfortunately, there were not enough participants to make statistically significant statements based on subjective computer knowledge or privacy importance. However, the diagrams showing the values have been included for completeness and can be found in figure 5 and figure 6. While the number of rejected policies does not deviate significantly between students and employed, the data reveals that students rate the importance of privacy lower than employed participants at 5.5 vs. $7.\overline{4}$ on a scale from 1 through 10.

4.3 Behavior

First and foremost we will take a look at the fake policy. While it has been rejected by 40% of all participants, it is unlikely that this was due to its actual content. The question at the end of the survey asked participants whether they noticed the fake text. Only one participant confirmed this, however, after reviewing the video footage it seemed unlikely that this person did do so. The popup was visible for less than two seconds. After receiving additional feedback from that participant it was revealed to be a mistake and that person meant to answer the question with no. Thus, no participant noticed the bogus text. This stands in stark contrast with subjective user behavior, where 31% claimed to consider the content of such policies. This reveals a discrepancy between the intended and actual behavior. Looking back at demographics, out of eight participants claiming to consider popups, half accepted four or more policies and these individuals valued the importance of privacy around the mid-point of the scale. This might indicate that some persons are in fact considering the popups but do knowingly decide to accept the policy. Whether or not this action stems from manipulation or other reasoning can not be determined from the data collected and requires more research.

Next, we will consider the consistency of individuals. For this, a fraction of accepted policies has been calculated for each participant and they have been accumulated in a histogram which can be seen in figure 3. Ten participants (40%) did consistently accept or reject policies. However, 60% did deviate from the extremes at least once with 28% doing so more than once. This indicates that a majority of users may not be following one logical strategy but are re-evaluating each time a website is being visited. With the deviation present, factors like popup design likely play a significant role in the users' choice. However, further research is required and a previous survey in this series of papers set the stepping stone for that [6].

Finally, we will take a look at individuals' behavior when interacting with a policy modal. To do so three categories have been defined. The first one is called "Evasive" and describes an interaction where the user dismisses a modal within seconds of it being displayed and does not interact with it in any meaningful way other than executing a single click. The second one is called "Normal" and describes an interaction where the user either takes more than five seconds or deviates from the direct path to dismiss the modal[10]. The last one is called "Persistent" and describes an interaction where a user thoroughly inspects a modal by clicking through multiple tabs, toggling multiple switches, or taking more than 30 seconds to dismiss it. Each interaction has been categorized and grouped by page.

[10]Which can be either rejection or acceptance. Clicking two buttons in quick succession to reject a policy is still considered "Evasive" if this is the fastest route to reject

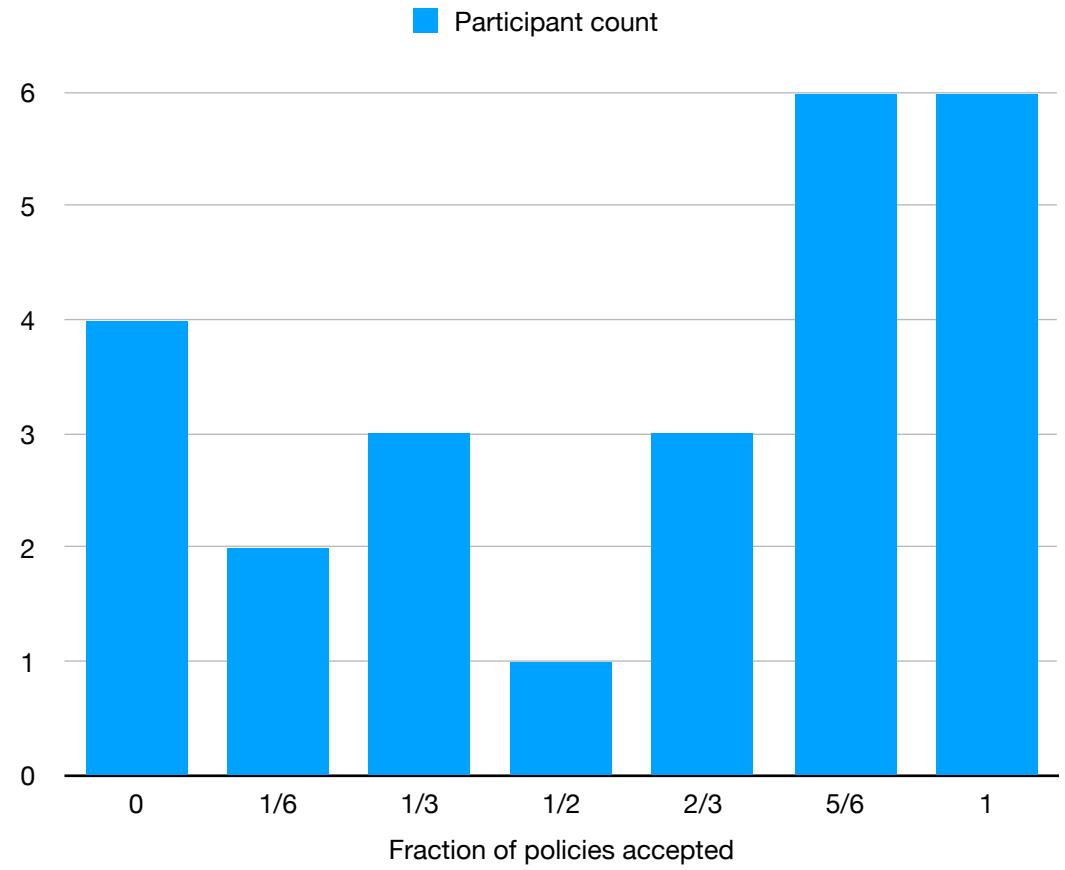

Figure 3: Distribution of user behavior regarding accepted policies

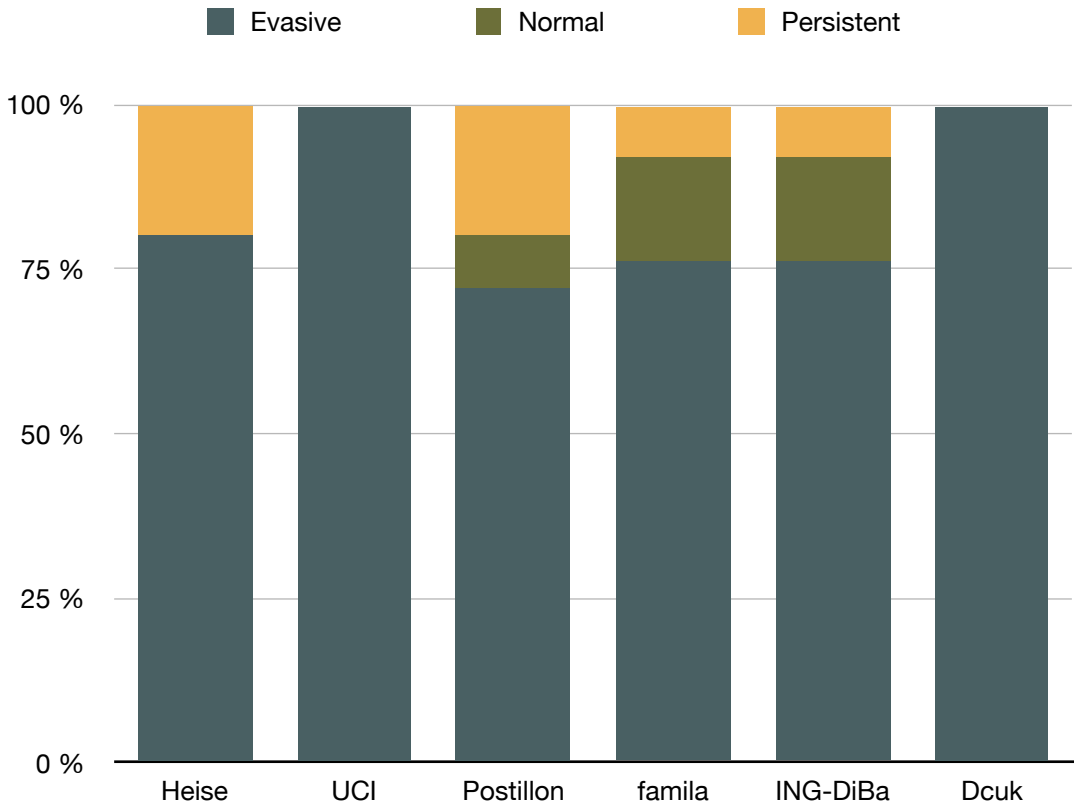

Figure 4: Behavior when interacting with a policy modal

The results are visible in figure 4. Note that the last page did not have any advanced configuration menus which might have adversely affected the number of persistent interactions. Overall, only 16% of interactions did not exhibit behavior which has been categorized as “Evasive”. It aligns with the results of a survey conducted in 2018 which showed that only ~11% of the participants do read the GDPR terms and conditions before giving consent [9]. This goes to show that a majority of user interactions happened quickly and without much consideration, indicating that users may have been conditioned to recognize the design and structure of privacy policy modals and take action to evade them to reach their desired information.

5 Conclusion

In this research paper, I have covered how the principle of operant conditioning works and what negative reinforcement is. Furthermore, I have analyzed the types of consent mechanisms present on the 300 most popular websites and developed a theory on how they could be used to condition users of the web. A survey has been designed and conducted with 26 participants which revealed evidence for conditioning taking place in the real world.

Additionally, the survey showed that most users do not stick to one strategy in dealing with privacy policies — either accepting or rejecting it — and uncovered that an astonishingly low number of persons do interact with such policy notices for a prolonged period. Virtually no participant did discover a faked modal during the survey, showing further evidence that users are only acting based on the known and trained structure of such modals instead of reading them carefully.

It remains questionable whether this effect of conditioning users into evading such consent workflows has been considered by the legislation in creating this policy. However, websites do profit from this phenomenon as a majority of users do not seem to act based on their preference leaving room to trick them into agreeing to share their data. This stands contrary to the original goal of the GDPR to protect the users’ data and privacy by default. Studies conducted in 2017 have shown that only 15% of IT decision-makers would support the claim that there are no drawbacks to the GDPR while 28% expected it to adversely affect the customer experience [10]. Overall it remains to be seen whether the new law does have any positive effects in this regard or drifts off to hinder the user experience at no gain in terms of privacy due to the unforeseen consequences of human psychology.

An unanswered question is what the motivations for accepting tracking and data collection policies are. It could yield insight into the reasoning behind the behavior exposed by this paper and how many users are aware of the permissions they give to websites. Furthermore, it remains unclear how many of the pages exhibiting no consent mechanism but are still tracking users. This could provide an outlook on how many websites are going to eventually add such consent workflows in the future, ultimately strengthening the effect of negative reinforcement.

Regarding the survey, a few notable discoveries have been made. Some users did circumvent/skip questions to which they knew the answer despite it being mentioned in the introduction. It seems that this instruction was unclear or skimmed over by participants. Following up on that, some users showed signs of distraction by not interacting with the survey for a prolonged period. This has probably been caused by the distribution method where users are participating in an uncontrolled, potentially noisy environment. Furthermore, some users were interrupted due to unstable internet connections. However, even with a stable internet connection, some websites did take a long time to fully load and present the modal. While it did not impact the survey results, it might very well cause issues in a larger survey.

Lastly, it may be noted that the survey did not match a 100% natural environment due to the difference in context and tasks. It remains possible that users do behave differently under more casual and/or natural circumstances.

Finally, the survey yielded vast amounts of data most of which have not been considered in this paper due to time and space restrictions. The survey design, although having some smaller flaws, did uncover interesting ways to analyze the data. However, with the low amount of participants, most results had to be abandoned. Thus, it might be of interest to conduct a similar survey in the future with a slightly shifted focus and at a larger scale.

Literature

[1] "The race to GDPR: A study of companies in the United States & Europe," Ponemon Institute, Apr-2018. [Online]. Available: https://iapp.org/media/pdf/resource_center/Ponemon_race-to-gdpr.pdf. [Accessed: 11-Oct-2020].

[2] "The history of the General Data Protection Regulation," European data protection supervisor. [Online]. Available: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en. [Accessed: 12-Oct-2020].

[3] "Regulation (eu) 2016/679 of the European Parliament and of the Council," Apr-2016. [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj. [Accessed: 02-Sep-2020].

[4] B. F. Skinner, "Two Types of Conditioned Reflex: A Reply to Konorski and Miller," *The Journal of General Psychology*, vol. 16, no. 1, pp. 272–279, Jan. 1937.

[5] B. A. Iwata, "NEGATIVE REINFORCEMENT IN APPLIED BEHAVIOR ANALYSIS: AN EMERGING TECHNOLOGY," *Journal of Applied Behavior Analysis*, vol. 20, no. 4, pp. 361–378, Dec. 1987.

[6] T. Blechschmidt, "Effect of cookie banner design on user click-through rate," Sep. 2020.

[7] "The Moz Top 500 Websites," 2020. [Online]. Available: https://moz.com/top500. [Accessed: 10-Oct-2020].

[8] D. J. Navarick, "Negative reinforcement and choice in humans," *Learning and Motivation*, vol. 13, no. 3, pp. 361–377, Aug. 1982.

[9] H. Tankovska, "Trust and vulnerability online: Consumers' practices and considerations related to GDPR in Norway 2018," p. 37, Dec. 2018.

[10] V. Bourne, "Opinion of IT decision makers on the drawbacks of the EU General Data Protection Regulations (GDPR) for citizens in Germany in 2017," May 2017.

Appendix

A Figures

All figures and screenshots below have been created/captured by the author for this research paper.

A.1 Graphs

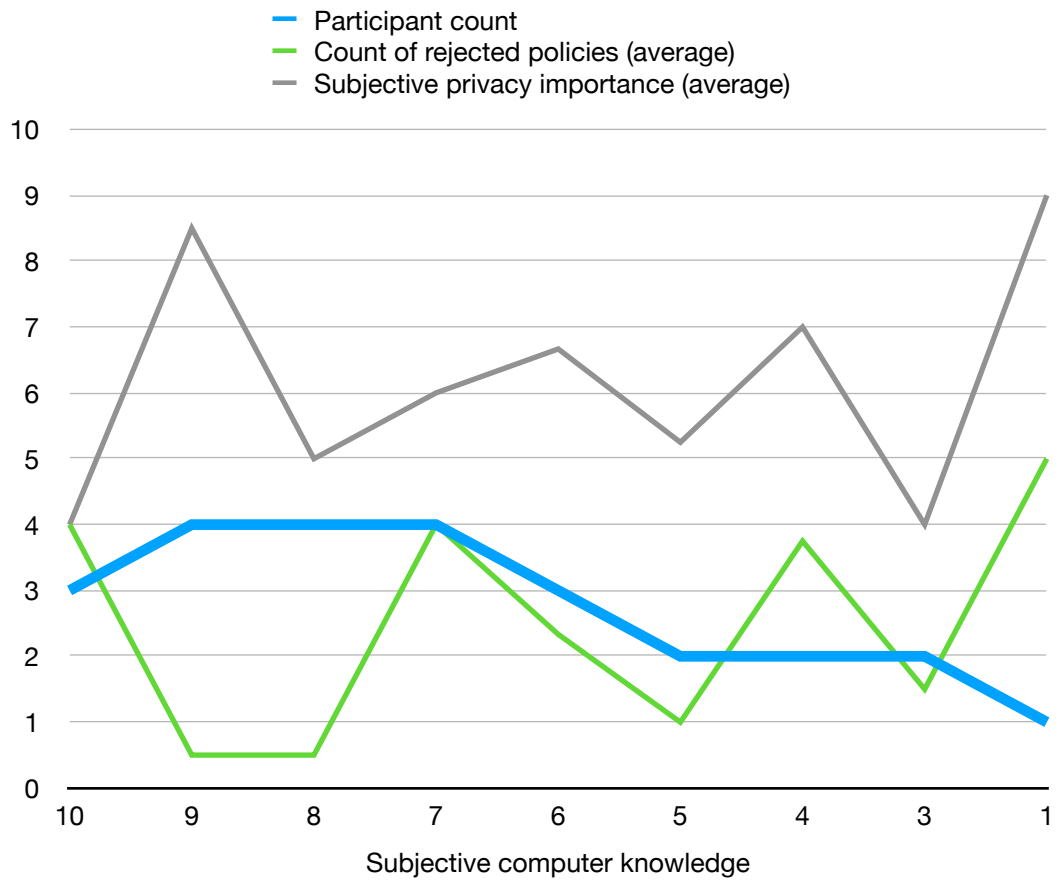

Figure 5: Demographics — Subjective computer knowledge

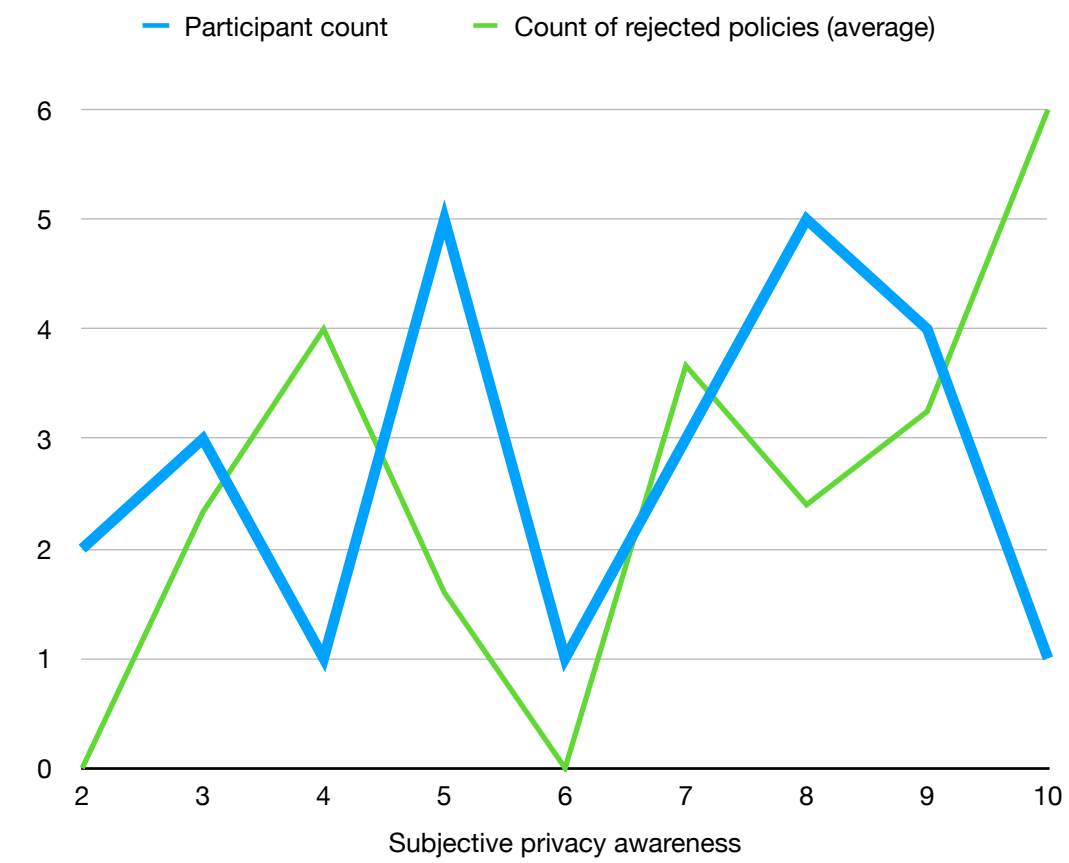

Figure 6: Demographics — Subjective privacy awareness

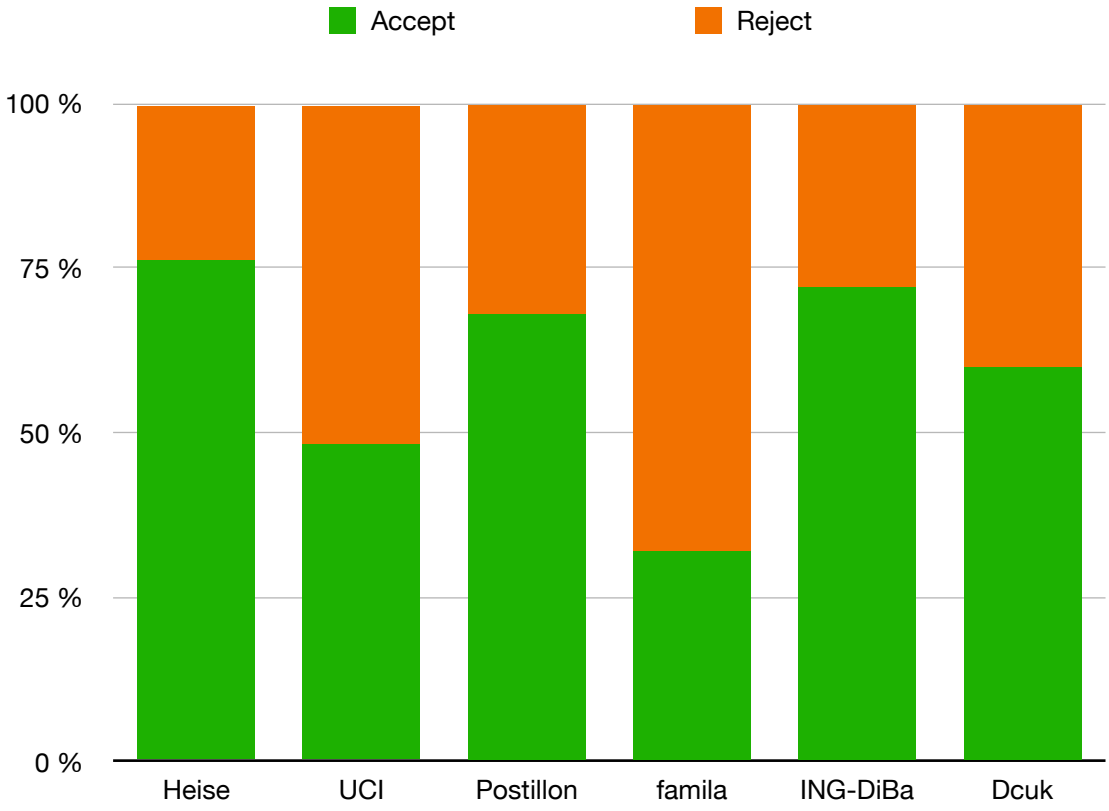

Figure 7: Actions taken regarding privacy policies (by page)

A.2 Screen captures

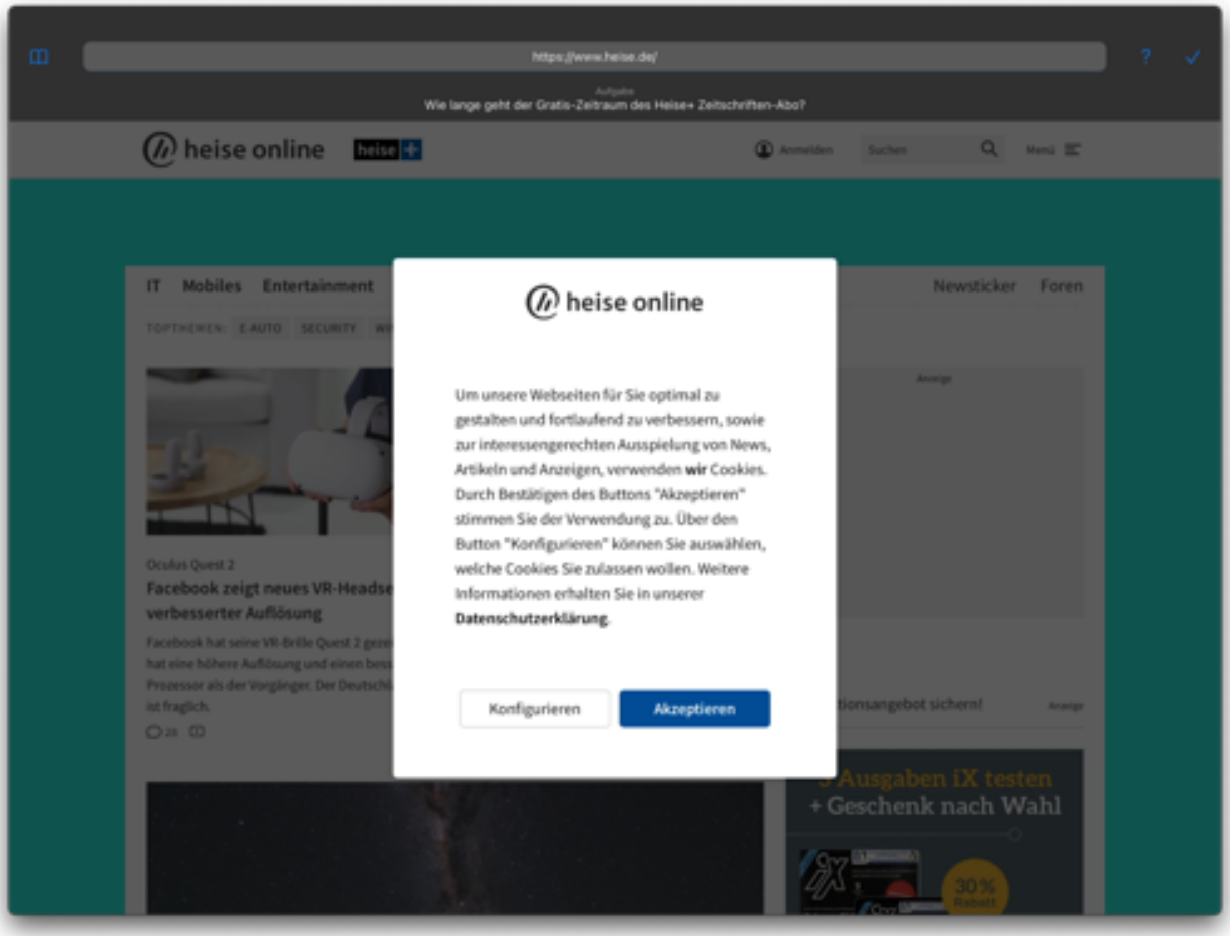

Figure 8: Website — Heise

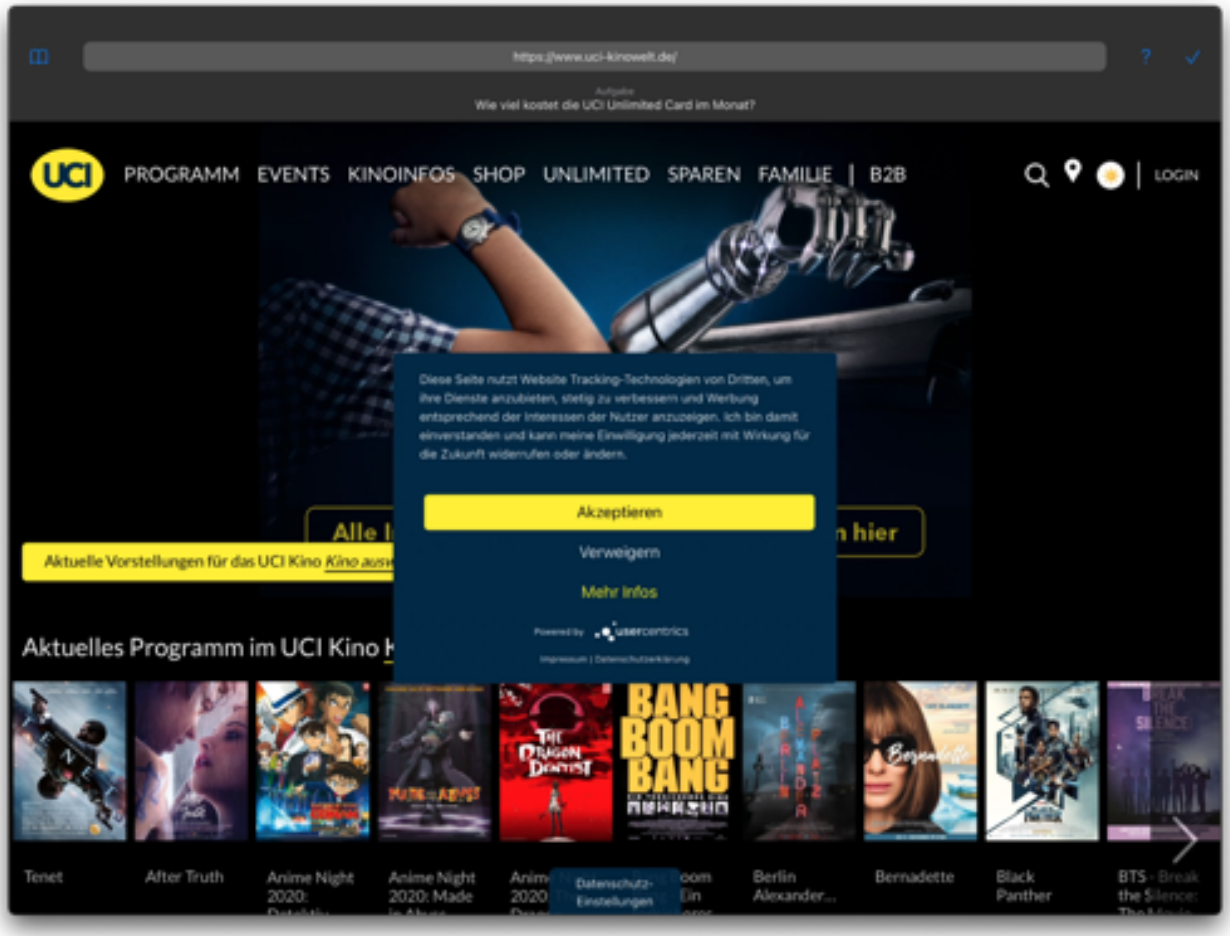

Figure 9: Website - UCI

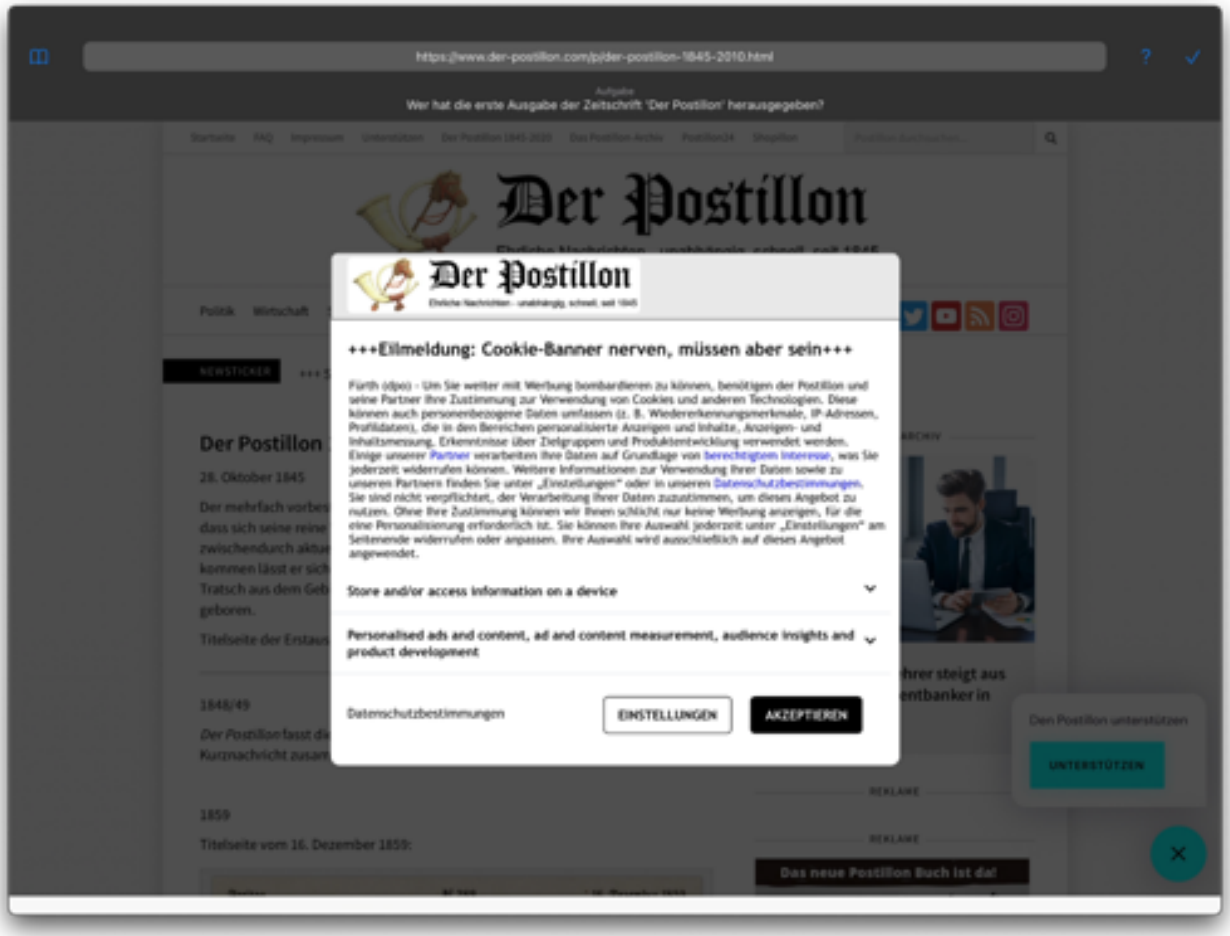

Figure 10: Website — Postillon

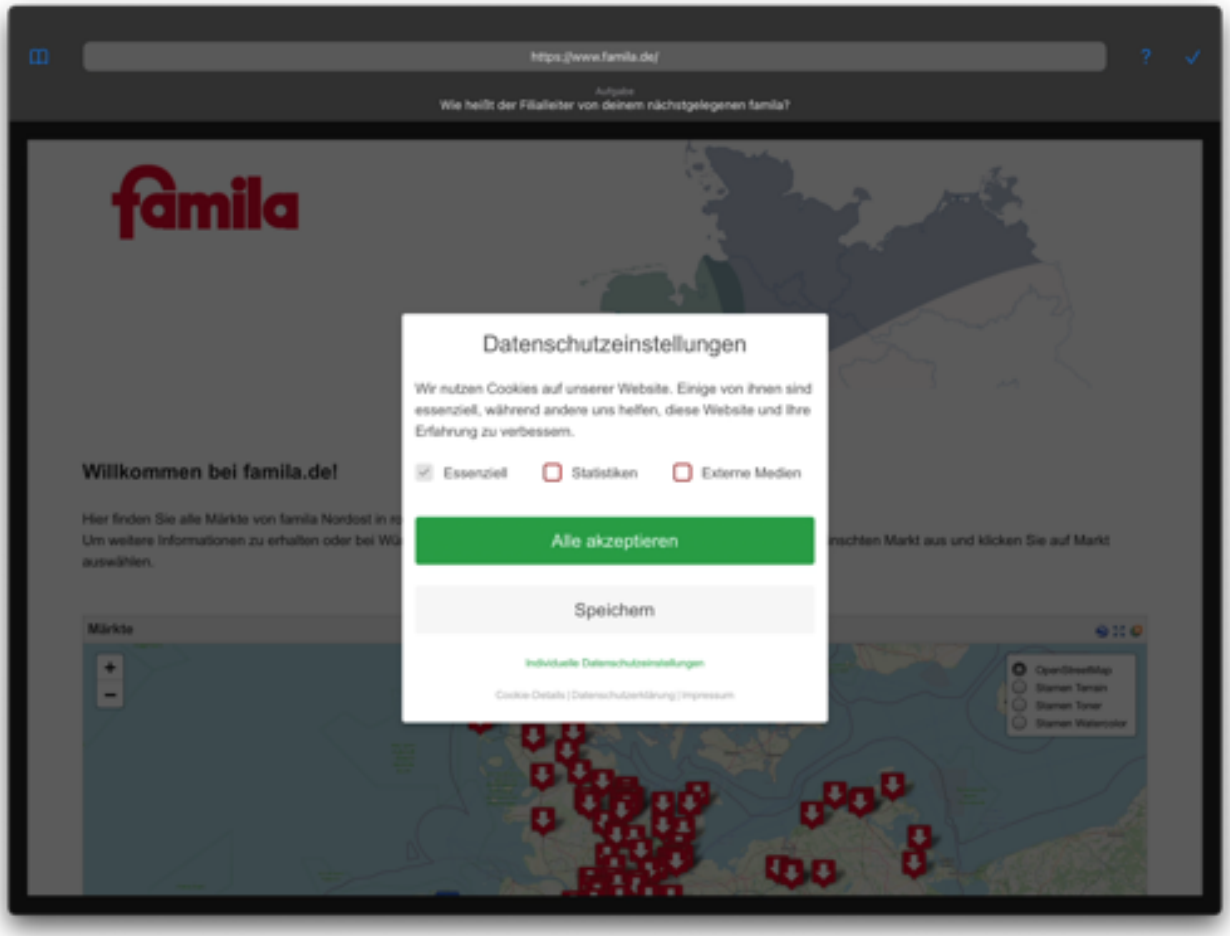

Figure 11: Website — famila

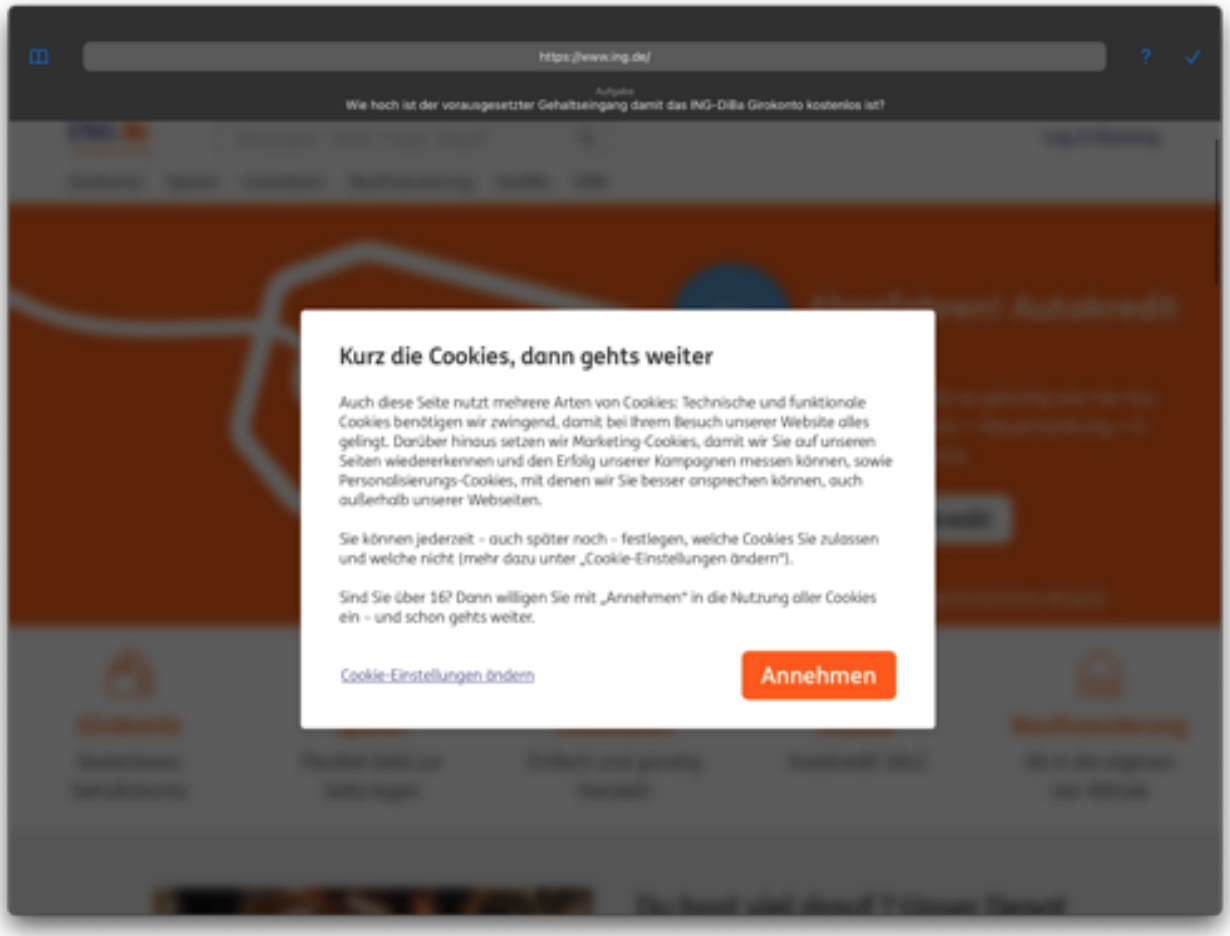

Figure 12: Website — ING-DiBa

Glossary

EU European Union. 1

GDPR General Data Protection Regulation. 1, 9, 11