Iowa State University
Digital Repository

Creative Components

Iowa State University Capstones, Theses and Dissertations

Spring 2021

Cookie for your thoughts: An examination of 21st-century design and data collection practices in light of Internet ethics and privacy concerns

Parth Shiralkar

Follow this and additional works at: https://lib.dr.iastate.edu/creativecomponents

Part of the Aesthetics Commons, Applied Ethics Commons, and the Management Information Systems Commons

Recommended Citation

Shiralkar, Parth, "Cookie for your thoughts: An examination of 21st-century design and data collection practices in light of Internet ethics and privacy concerns" (2021). *Creative Components*. 811.
https://lib.dr.iastate.edu/creativecomponents/811

This Creative Component is brought to you for free and open access by the Iowa State University Capstones, Theses and Dissertations at Iowa State University Digital Repository. It has been accepted for inclusion in Creative Components by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

المنارة للاستشارات

www.manaraa.com

Cookie for your thoughts: An examination of 21st-century design and data collection practices in light of Internet ethics and privacy concerns

by

Parth Shiralkar

A Creative Component submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Systems

Program of Study Committee:
Dr. Anthony M. Townsend, Major Professor
Dr. Jonathan Y. Tsou

The student author, whose presentation of the scholarship herein was approved by the program of study committee, is solely responsible for the content of this dissertation/thesis. The Graduate College will ensure this dissertation/thesis is globally accessible and will not permit alterations after a degree is conferred.

Iowa State University

Ames, Iowa

2021

Copyright © Parth Shiralkar, 2021. All rights reserved.

للاستشارات المنارة

www.manaraa.com

DEDICATION

I would like to dedicate this dissertation to my parents, without whose consistent and unyielding support, I would not have been able to complete this work. I would also like to dedicate this work to myself - completing this research is a proud achievement.

المنارة للاستشارات

www.manaraa.com

TABLE OF CONTENTS

المنارة للاستشارات

www.manaraa.com

LIST OF FIGURES

المنارة للاستشارات

www.manaraa.com

ACKNOWLEDGMENTS

I would like to take this opportunity to express my thanks to those who helped me with various aspects of conducting research and the writing of this thesis. First and foremost, Dr. Anthony M. Townsend for his guidance, patience and support throughout this research and the writing of this dissertation. His own research in the field of human-computer interaction has often inspired me, and his words of encouragement have bolstered my confidence in completing this work. I would also like to thank my other committee member Dr. Jonathan Y. Tsou, under whose excellent direction I carried out the independent research that would build the foundation for this dissertation. His insights regarding the philosophy of technology have been instrumental in my studies.

المنارة للاستشارات
www.manaraa.com

ABSTRACT

Following the rapid growth of the Internet and the industries stemming from it, philosophical theories have sought to argue for more limits on contemporary surveillance practices and information gathering. These theories attempt to discuss the handling of personal information. In modern times, information is gathered through a wide range of sources and methods and then processed - this data goes through a gauntlet of processes: it is manipulated, shared (sometimes for a fee or a barter), and treated, becoming part of the Internet economy – the financial ecosystem of the Internet (Davenport et al., 2001).

Keeping in mind the intricate relationship between privacy and the sphere of public knowledge, this dissertation aims to a) examine the current state of the data collection practice in light of a historical record of privacy and ethics discourse that dates as far back as the very inception of the Internet (Moore, 2003), and b) propose a proactive framework that companies (and even governance institutions) could utilize for further development in these sectors. I will use theories and studies from my research over the past year to discuss the current situation of the data collection industry in the United States. Over the course of this paper, I shall then argue that although digital privacy has been deemed important since the Internet came into existence (Flanagan et al., 2008), it bears a certain disconnect with current industry practices. This paper will also discuss why, with the incredible pace of technological advances, commensurate legislation for data mining seems unable to keep up. In the final section, I propose a framework that could serve as a guideline for additional policy design.

Keywords: cookie banner, personal data, internet ethics, user experience, privacy by design

المنارة للاستشارات

www.manaraa.com

CHAPTER 1. The Age of Surveillance

Technological advancements come in phases (Almgren and Skobelev, 2020), and it would be safe to assume that the next phase will bring with it a slew of fresh privacy concerns. Data collection began as a simple process of recording basic consumer data; now, information aggregation is a multi-million-dollar industry. The FAANG (Facebook, Apple, Amazon, Netflix, and Google) corporations, which are rightly considered the industry leaders in their domains, are built on the backbone of the data economy (Athique, 2020). More cutting-edge developments in IoT, A.I. and augmented reality infrastructure, will create opportunities for improved target reach, a better understanding of consumer bases, and new data collection methodologies. With this, the marketing industry will seek out an edge over the competition – this will be in the form of widespread strategies that encompass every conceivable form of media. A virtual universe, rife with advertisements. The market will no longer be confined to the 2D world of printed flyers; 3D, immersive marketing will be part of the new wave (Wedel et al., 2020).

1.1 Introduction

1.1.1 A Data-driven World is Inevitable

In its current state, the privacy policies governing the usage of and engagement with most major IT structures, software components, apps, etc. are fundamentally based around the concept of allowing users to explicitly take away consent after said consent is automatically assumed by continued usage of the app/website/software (Papadogiannakis et al., 2021). This, I think is one of the hard cores of the idea of privacy, and thus should be given appropriate consideration. And so, this paper shall attempt to answer the following questions: How well does the current privacy policy standard hold up in context of the various definitions of privacy? And if there is indeed room for improvement, what's a good place to start? Past research suggests not

www.manaraa.com

only that most End User License Agreements ("EULAs") currently in use across the world are lacking in transparency (Pollach, 2005), but also that some of these EULAs are deliberately designed with malicious intent (Machuletz and Böhme, 2020). With examples of cookie policy notices/banners (among other cases), I shall argue for a reexamination of the notions of sharing personal data. In the following sections, other aspects of the data collection industry that contribute to the generally opaque nature of the data collection processes will be discussed. Finally, the proposed framework shall be discussed, focusing on aspects concerning corporations and government bodies alike.

1.1.2 The Ease of Data Aggregation is a Factor

The processing of information in an electronic format is a highly convenient method of data aggregation. Huge collections of data (databases) and huge collections of databases (data warehouses) can be searched in real-time at high speeds, and large quantities of information can be manipulated in batches (Solove, 2004). According to studies over the past two decades, data can help inform important decisions and actions (Davenport et al., 2001), and can be modeled and leveraged to generate insights for future decisions.

Especially in 2021, database management techniques are being optimized to handle what seems like an endless supply of data (Doss, 2020). This surge in data management techniques, coupled with the improvements in data collection and aggregation methodologies, brings about the need for a fresh discussion about these techniques. In her book, Helen Nisenbaum discusses their "capacity to extract descriptive and predictive meanings from personal information that goes well beyond its literal boundaries" (Nissenbaum, 2004a). Before the internet, data collection relied mainly on surveying people - now, most data aggregation techniques are automated. For example, by simply agreeing to use a website, internet users also agree to cookie usage over that website's domains. Indeed, these are powerful techniques, and they will continue to grow in efficacy and speed (DeCew, 2018).

المنارة للاستشارات
www.manaraa.com

CHAPTER 2. What Does Privacy Mean? Why Does It Matter?

With the invention of the Internet, the definition of privacy was altered to accommodate the virtual world that the Internet had brought about (Moore, 2003). Around sixty years ago, when the Internet came into existence, it made a lot of things easier, including the collection of data. Detailed information about thousands of individuals could be collected, stored, and processed for cheap, with little strain on available resources (Davenport et al., 2001; Bataineh et al., 2020). With this ease, there has been a natural attempt by defense sectors of the government, and other massive conglomerates of the time, to call first dibs on the most advanced developments in the growth of the Internet (Doss, 2020). The swift technological progress in terms of data collection we're making is met with mixed reactions from the general public. One side believes that privacy in this age is a myth, and that we should adapt to the wave of invasive technology. The other side wants to protect and preserve our privacy, now more than ever, when data collection is the norm and privacy is just a setting (Moor, 1997).

2.1 The Legal and Non-legal Importance of Privacy

In a 2004 paper, Helen Nissenbaum claims that information technology is essentially implicated in the relentless gathering of information (Nissenbaum, 2004b) by companies that manage massive databases of user data. She suggests that this is due to the immense capability of information technology to contain data so swiftly and cheaply. The invention of a virtual world and these fast, low-maintenance data management techniques can be considered instrumental in the evolution of the Internet age. Powering through the initial developmental stages, the Internet has grown popular as an invaluable resource, and analysts and writers only contributed to this burgeoning popularity. This has, indeed, forced scholars to question previous notions of privacy (Smith and Dinev, 2011). Theorists have tried to define privacy in several ways over the years,

المنارة للاستشارات
www.manaraa.com

even before the Internet existed. Of course, the debate over whether privacy is a coherent concept or not has been going on for years as well (DeCew, 2018).

2.1.1 Definitions of Privacy in the Context of Law and Philosophy

Even though the definitions of privacy have seen changes through the years, alongside the technological advancement of the Internet itself, I believe that there is an inherent value to personal, private space, whether online or offline.

2.1.1.1 Privacy is of Value

Theorists have spent years trying to determine if privacy has innate value. Adam Moore's views on privacy build greatly on the fundamental analysis of privacy by Ruth Gavison (Moore, 2003; Gavison, 2011). According to these theorists, privacy, especially in the context of the existence of the Internet, is a relative concept, not an absolute one (Gavison, 2011). I am inclined to agree with this claim.

Consider an individual detached from society. If there is no one else around this individual to hide anything from (or, more accurately, keep something private from), there's no reason for the idea of "privacy" to hold much importance. *We live in a society*, and among the many implications of that statement is the inevitable interaction between members of said society. There have been other theories that discuss other aspects of the concept of privacy (Tavani, 2007), but this paper will attempt to examine some more technologically-relevant ideas. Moore goes on to describe a kind of control over access to information about oneself when interacting with society (Moore, 2003). That, I believe, is one of the core ideas of privacy, which I hope to explore in this dissertation.

Other thinkers including Ruth Gavison and Anita Allen have discussed this as well, claiming that having a level of control over sharing information pertaining to details of individuals is important (Gavison, 2011). I believe this line of reasoning is the most compelling one for a reconsideration of current Internet-based privacy laws for the following reasons: 1) When Internet

المنارة للاستشارات www.manaraa.com

users enter data on websites and apps, this data (details like first and last name, birth date, general interests, etc.) gets entered into databases, where the processing begins. This is typically the point at which users start losing control over what happens to their data. 2) When users start to lose control over the flow of information, it affects their privacy (Yu et al., 2020). I argue for better ways to let users control the flow of their own data, in a way that can be beneficial to corporations, with the user's **explicit** permission. I highlight the word "explicit" because of the implicit assumption of user consent, which I'll discuss in a further section. Thus, among the various theories applicable to privacy, where the digital age is concerned, the theories that focus on the flow of information, and the idea of consent, are the most relevant.

2.1.2 Legal Definitions and their Implications

In this section, I shall discuss some prominent definitions of privacy - especially in light of the Internet's wide reach and the disconnect between the concept of personal data and current industry practices.

2.1.2.1 Western Law should be Re-examined

Laws that govern personal data and privacy tend - especially in the USA – to be based around the idea of bad persons in the midst of good persons (Floridi, 2014). According to Floridi, the government is on the prowl for Moby Dicks (bad persons who commit illegal activities) while their net is cast over the shoal of sardines (good persons). A fierce proponent of Open Data collectives, Floridi makes compelling claims to urgently update the law in order to better protect persons, and even groups of persons. There is a disconnect between the laws that govern privacy and the technological advancements that affect privacy, and thus personal data (Nissenbaum, 2004a). While laws regarding email collection were being established, technology that could track individuals in the real world was already being developed. When it comes to privacy policies, most Western legal systems follow a general guideline framework as follows (Gavison, 2011), to ensure that:

المنارة للاستشارات
www.manaraa.com

1. The data being collected is accurate
2. Individuals know what information is being held in data banks
3. The acquisition and dissemination of information are controlled

While the measured process of obtaining and processing the information is a good practice privacy-wise, note how the first two have nothing to do with privacy. 1. The data being accurate will not allow the individual to control it. I believe this step is part of common guidelines to assuage the fears of individuals (Yu et al., 2020). The user can, of course, take solace in knowing that certain details of their life have been documented accurately, but this knowledge does not help their inability to control what happens to the information as a whole. 2. Knowing what information is being collected, could – in some cases – be worse for the individuals. The knowledge of some confidential aspect of their life being collected could be enough to send them into a state of panic. Consider an example: A publicly religious individual downloads a secretive dating app on their phone. At the time of installation, the app manager lets them know that the app will collect their full name and some other personal information - their association with the app is now part of some collected data that they know nothing about. On the other hand, to the data brokers and database managers it would appear that as long as the data banks are functioning normally, the individual's privacy does not warrant consideration.

2.1.2.2 A Disconnect Between Ideas

In "Managing Privacy" by H. Jeff Smith, the disconnect between a desirable measure of "privacy" is discussed in light of company privacy policies about data collection (and sharing) (Smith, 1994). For the sake of this discussion, all kinds of company-drafted and –issued cookie policies, tracking clauses, so on, can be collectively termed "privacy policies." In his book, Smith says that companies typically do not follow a shared template when they draft their privacy policies. Though the underlying message is similar ("yes, we are aware of the privacy problem"), the specific policies may differ greatly from company to company. What company A might allow

www.manaraa.com

its data brokers to do with the data could be completely different from what company B allows it data brokers to do. The data could virtually be sold and traded around the world without the user ever knowing it (Athique, 2020). I claim that these privacy policies involve a deliberate attempt to be lenient in certain areas - data collection in particular. When we see companies like Instagram and Facebook making use of muscle memory (Liu and Yang, 2020) to drive traffic to their products, it prompts the consideration of other companies (e.g. non-profit open-source software developers like https://fossdroid.com/ and https://f-droid.org/) that offer apps without these tricky pitfalls.

My reasons for this claim also stem from the existence of companies that make an effort – a visible attempt at clarity. The very fact that some companies are taking efforts to make sure they are transparent in their policies, makes it highly unlikely that Instagram's new design principles are a fluke. To add on to this argument, see Figure 3.1 - note the clear distinction between permission windows, setting privacy preferences, so on. Frequently, the company privacy policies have no backbone, no underlying "right to privacy", instead relying on public support and viewer perception for relevance (Smith, 1994). Companies today are not concerned with "privacy" itself, but with the notion that their customers view their corporate image as "privacy-conscious".

2.2 A Dubious Alternative

Some might argue for another option: going "off-the-grid" entirely – I believe such measures are simply not feasible for everyone. The Internet is a necessary utility, and for the majority of its users, going off-grid is not an option. Even if the average user were to attempt this, they might lose contact with their close family and loved ones. Despite these efforts, the only person benefiting from this would be the individual. While not impossible, this approach is not a viable option for everyone. I do not think that getting rid of all technological equipment in an act of defiance would be particularly useful against the wide reach of the technology itself. Once again, I argue for a reconsideration of the relationship between the current data collection policies of most Internet-based companies and the concept of assumed consent.

المنارة للاستشارات
www.manaraa.com

CHAPTER 3. Modern Design Principles - Bypassing Consent

3.1 Introduction

The disconnect discussed in the earlier section is an important statement to be made, I think, where companies like Instagram (owned by Facebook) roll out updates to their apps with a certain motive in mind: these updates contain changes to the user interface that designed to make use of muscle memory (Carman, 2020), thereby having users involuntarily click on certain sections of the app. I believe that these changes are made with sinister purposes, and that moving the buttons around may seem like a trivial change at face value, hiding the more subtle changes at a deeper level (Nouwens et al., 2020). For example, let us consider one of Instagram's newest features: the shopping tab. Instagram has a "likes and activity" tab which used to be at the bottom right of the homepage. Easily accessible by a simple thumb movement, this tab was one of the most commonly used tabs on the app. Since the new update rolled out, its current location is at the top of the screen, and its original position has been taken up by the shopping tab. Discussion forums all over the internet were rife with disdain over this new change (Carman, 2020). Perhaps these are all marketing ploys on the surface, but the little tricks that prey on unsuspecting users are unnecessary at best, and in poor taste when it comes to safeguarding privacy (Handayani et al., 2018; Matte et al., 2020; Soe et al., 2020).

3.1.1 Websites Try to Bypass Consent

As of recent, the norm in data collection industries is heavily biased towards opt-out consent gathering (O'Connor et al., 2020). What this means is, users are automatically opted into the cookie policies and other EULAs, simply by using the website, even simply navigating from one webpage to another. This is a very tricky aspect when the idea of consent comes into play: a huge part of this is metadata (Bauer et al., 2021). Metadata is the data about data, a big part of the

المنارة للاستشارات
www.manaraa.com

overall file structure of cookies. In an earlier section, I discussed the technological workings of cookies. In this section, I shall discuss the idea of assumed consent that this metadata is at odds with.

3.1.1.1 Cookies and Consent

The metadata saved inside any random cookie can contain information about the make and model of the user's machine, their last saved location, websites visited (including the type of websites visited), details of the internet traffic over the machine's network cards, generally content that can be used to classify users into categories. Some special types of cookies can also be used to keep track of a device's location in real-time, thus leaving open a large number of potentially dangerous uses (Papadogiannakis et al., 2021). Many users are yet unaware of what exactly these cookies do (Bornschein et al., 2020).

I believe here that the problem with assumed consent is two-fold: 1.) Most users do not know what exactly it is that the cookies do. 2.) Even if they do know what the cookies do (and that it is prudent to disable them) they have to take extra steps to disable them. What users think of when they see "cookies" is a general mix of indifference and ignorance, as can be seen in a 2020 study (Bellentani, 2020). A quick survey of cookie knowledge among my peers revealed that only those with a background in IT had any clue about the workings of the cookie. Recent research has opened up the forum to questions regarding the nudges towards accepting cookies by websites that use these cookie banners to an advantage (Matte et al., 2020). I'm using cookies as an example here because of their status as one of the most basic web tracking technologies (Palmer, 2005).

3.1.1.2 Agree to Disagree: Dialog Boxes

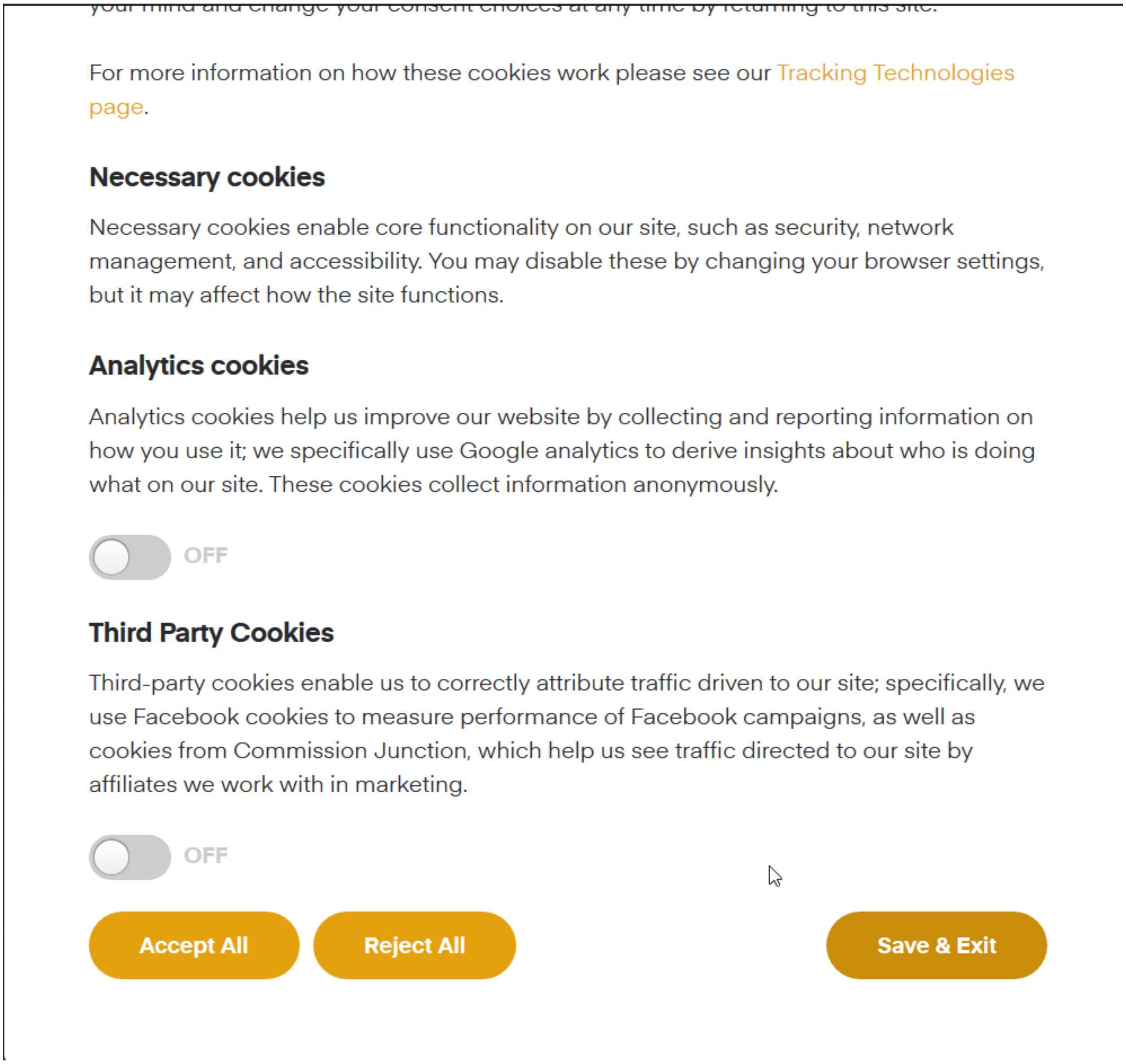
According to studies in the past five years, there is a visible difference between the two sides of the cookie settings on most websites: the part which prevents specific tracking cookies from being generated, and saved and the part which allows all cookies on the website (Soe et al., 2020; Matte et al., 2020). I'll be discussing the design challenges in these cookie settings windows in a

المنارة للاستشارات
www.manaraa.com

following section, but for this part, let us examine the ease of tweaking the default cookie settings of websites. In Figure 3.3, it is simply more convenient to say ”I Agree” and move on, than chasing down the specific setting to opt-out of sharing cookies and other personal data. Because of the default assumption of consent, the burden of making sense of the website’s cookie/privacy policies is suddenly on the users themselves. When users first visit a website, they are greeted by some pop-ups and notices regarding the website’s terms. A typical such notice will be worded somewhere along the lines of **“By continuing to use this website, you agree to the website’s Terms & Conditions and Privacy Policies, including the Cookie Policy. To make changes to the cookie settings of this website, please visit the privacy policies of our marketing affiliates.”** (Bornschein et al., 2020) And thus, the user is sent on a wild goose chase to disable the cookies, as can be seen in Figure 3.2.

المنارة للاستشارات
www.manaraa.com

3.2 Figures



your mind and change your consent choices at any time by returning to this site.

For more information on how these cookies work please see our Tracking Technologies page.

Necessary cookies

Necessary cookies enable core functionality on our site, such as security, network management, and accessibility. You may disable these by changing your browser settings, but it may affect how the site functions.

Analytics cookies

Analytics cookies help us improve our website by collecting and reporting information on how you use it; we specifically use Google analytics to derive insights about who is doing what on our site. These cookies collect information anonymously.

OFF

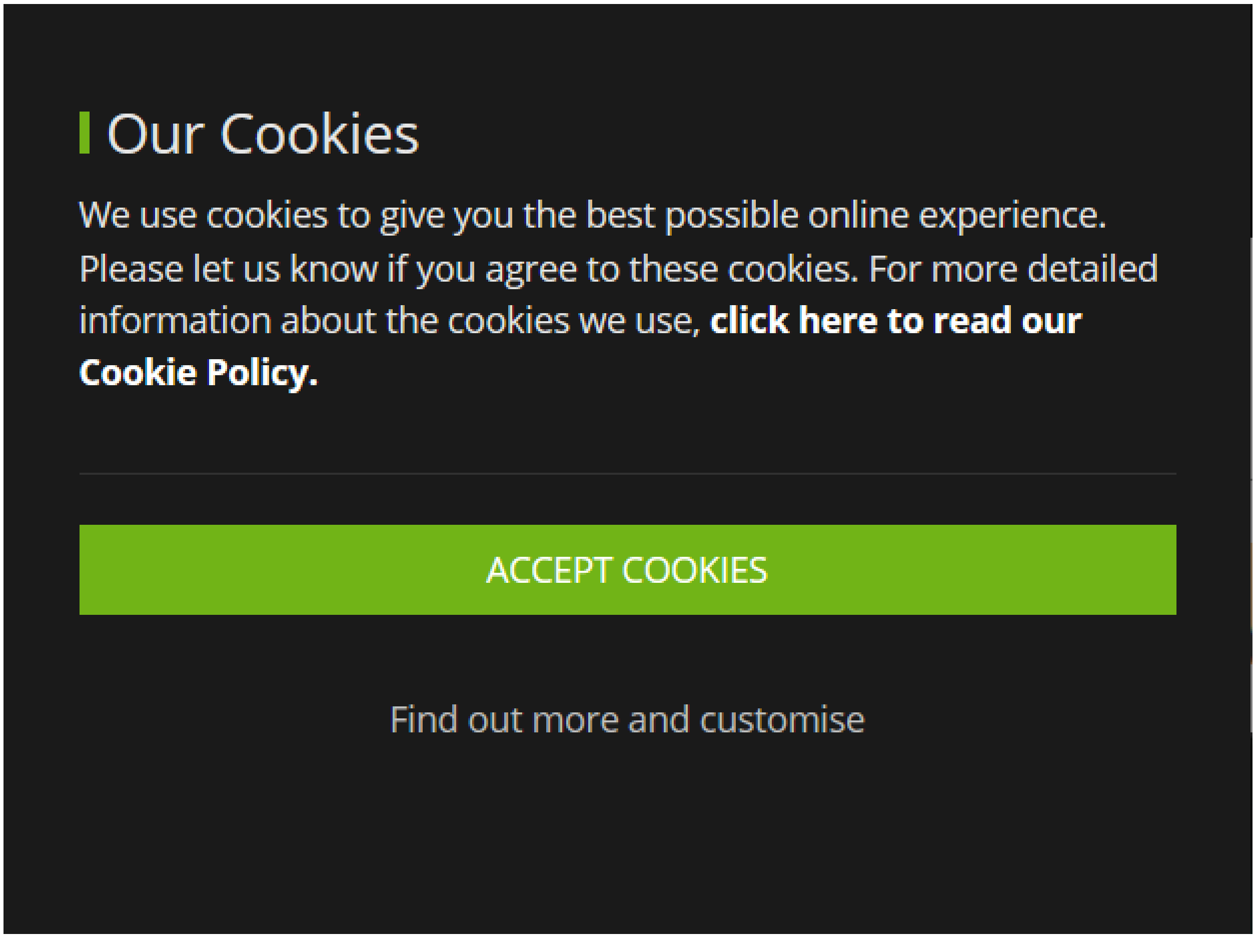
Third Party Cookies

Third-party cookies enable us to correctly attribute traffic driven to our site; specifically, we use Facebook cookies to measure performance of Facebook campaigns, as well as cookies from Commission Junction, which help us see traffic directed to our site by affiliates we work with in marketing.

OFF

Figure 3.1 Concise cookie preferences

المنارة للاستشارات
www.manaraa.com

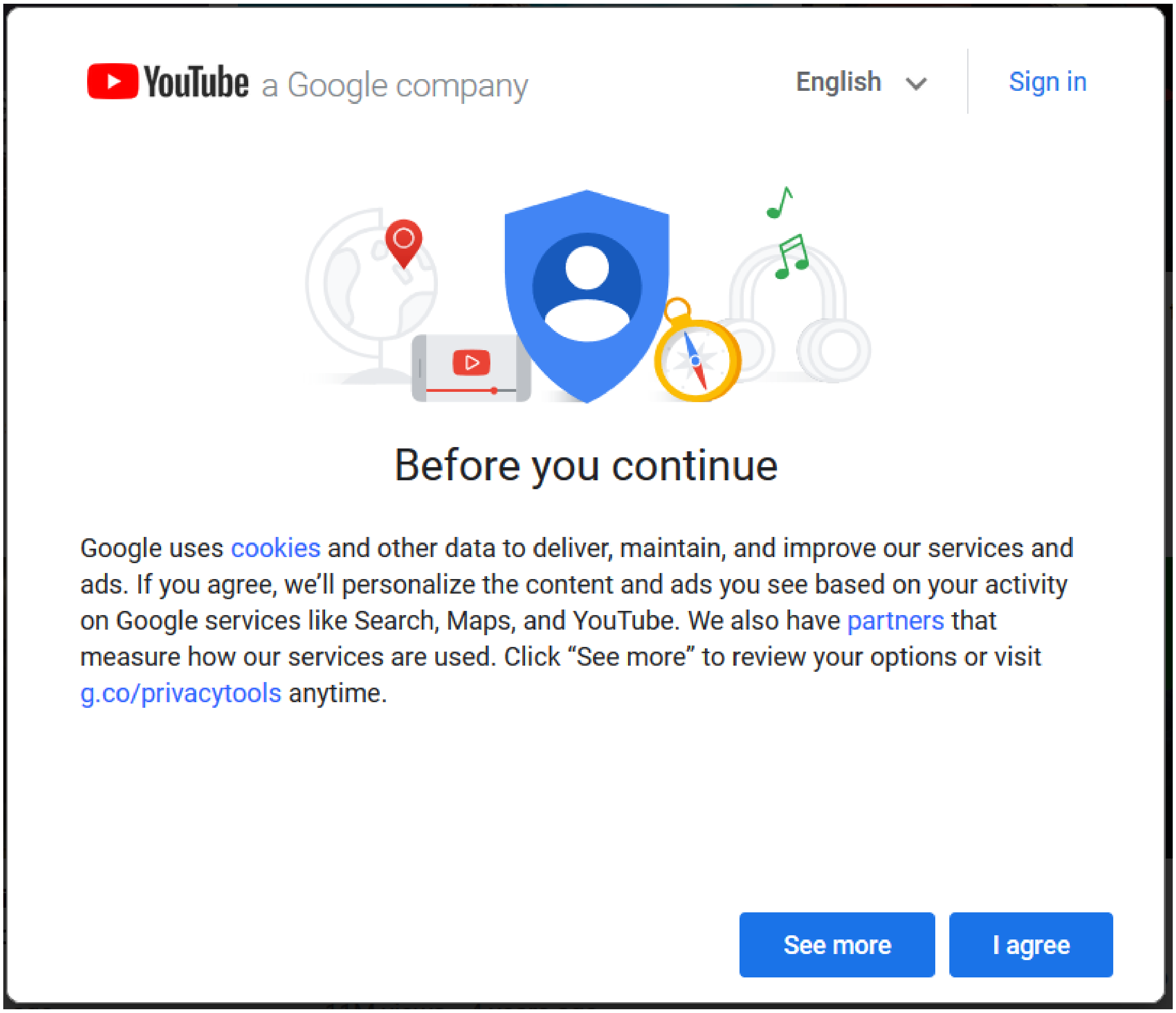


Our Cookies

We use cookies to give you the best possible online experience. Please let us know if you agree to these cookies. For more detailed information about the cookies we use, **click here to read our Cookie Policy.**

Figure 3.2 Very prominent "Accept Cookies" button

المنارة للاستشارات
www.manaraa.com



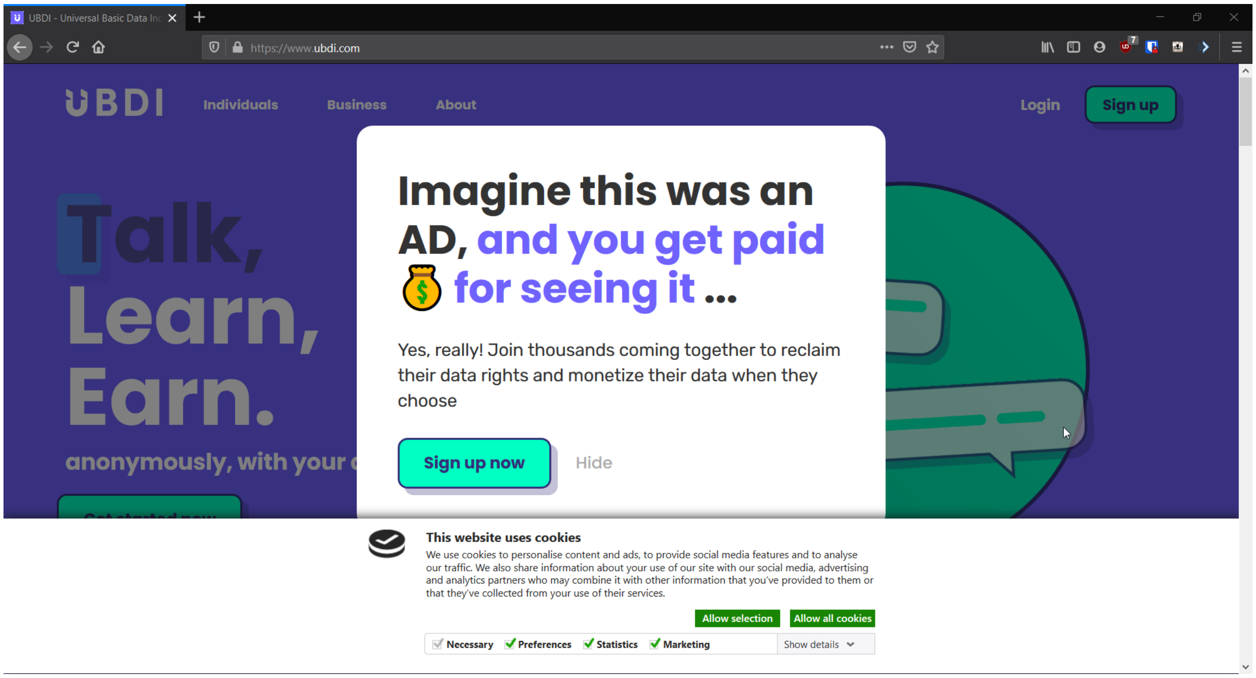
Before you continue

Google uses cookies and other data to deliver, maintain, and improve our services and ads. If you agree, we'll personalize the content and ads you see based on your activity on Google services like Search, Maps, and YouTube. We also have partners that measure how our services are used. Click "See more" to review your options or visit g.co/privacytools anytime.

Figure 3.3 Only "I Agree" on this page

المنارة للاستشارات

www.manaraa.com



Imagine this was an AD, and you get paid 💰 for seeing it ...

Yes, really! Join thousands coming together to reclaim their data rights and monetize their data when they choose

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you've provided to them or that they've collected from your use of their services.

Figure 3.4 Giving the power back to the user

المنارة للاستشارات

www.manaraa.com

CHAPTER 4. Observations and A Proposed Framework

It is clear that the current industry practices - especially in modern UI-based dsign - are not completely in line with user-centric data governance policies like the GDPR (Graßl et al., 2021; Machuletz and Böhme, 2020). Relevant research in the general area of privacy has been around for long, but the modern design principles of websites are in a nascent stage of study (Doss, 2020). Studies are still attempting to examine the nature of technological products and services in the context of ethical standpoints (Flanagan et al., 2008; Tavani, 2007).

As such, I submit a structured approach to evaluate design practices and privacy policies. The framework I propose is a structure of three main areas of focus to ensure viability of policies and guidelines. The three cores of the framework are as follows:

1. **Opt-in over Opt-out**
2. **Autonomy**
3. **Transparency in Design**

This framework is meant as a simple guideline - I have attempted to identify and simplify the foundation of privacy concerns in UX/UI design. The three main factors at play in this framework are consent, autonomy, and clarity.

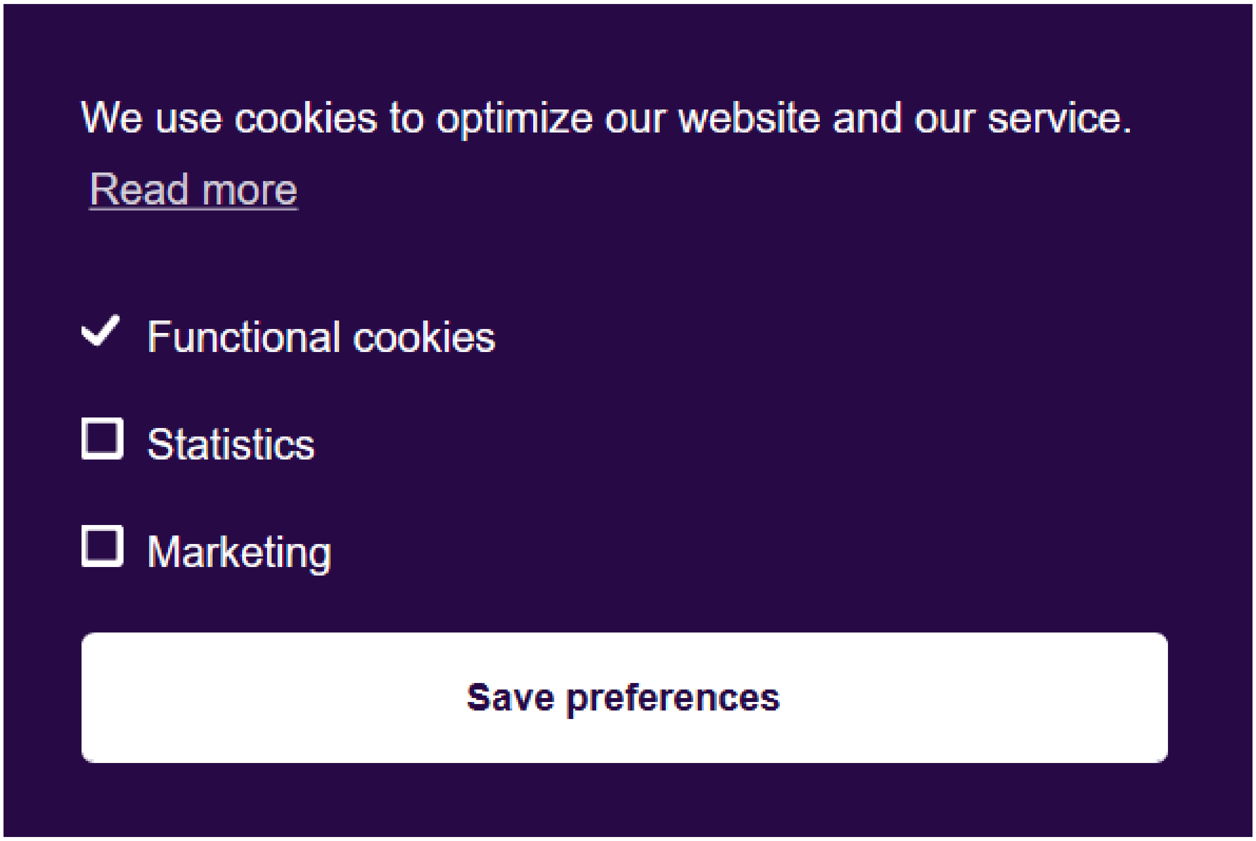
4.1 Opt-in over Opt-out

In the previous section, it was seen how users can be nudged into accepting all cookies by default, and then the only remaining option is to find the opt-out settings. I believe that the first step in the pushback against intrusive design would be ensuring that the default settings are opt-in, and not opt-out. Research suggests that users are currently not being exposed to the best

المنارة للاستشارات

www.manaraa.com

practices in UX design, thus preventing them from making meaningful choices when it comes to the sharing of personal data (Graßl et al., 2021).



We use cookies to optimize our website and our service.

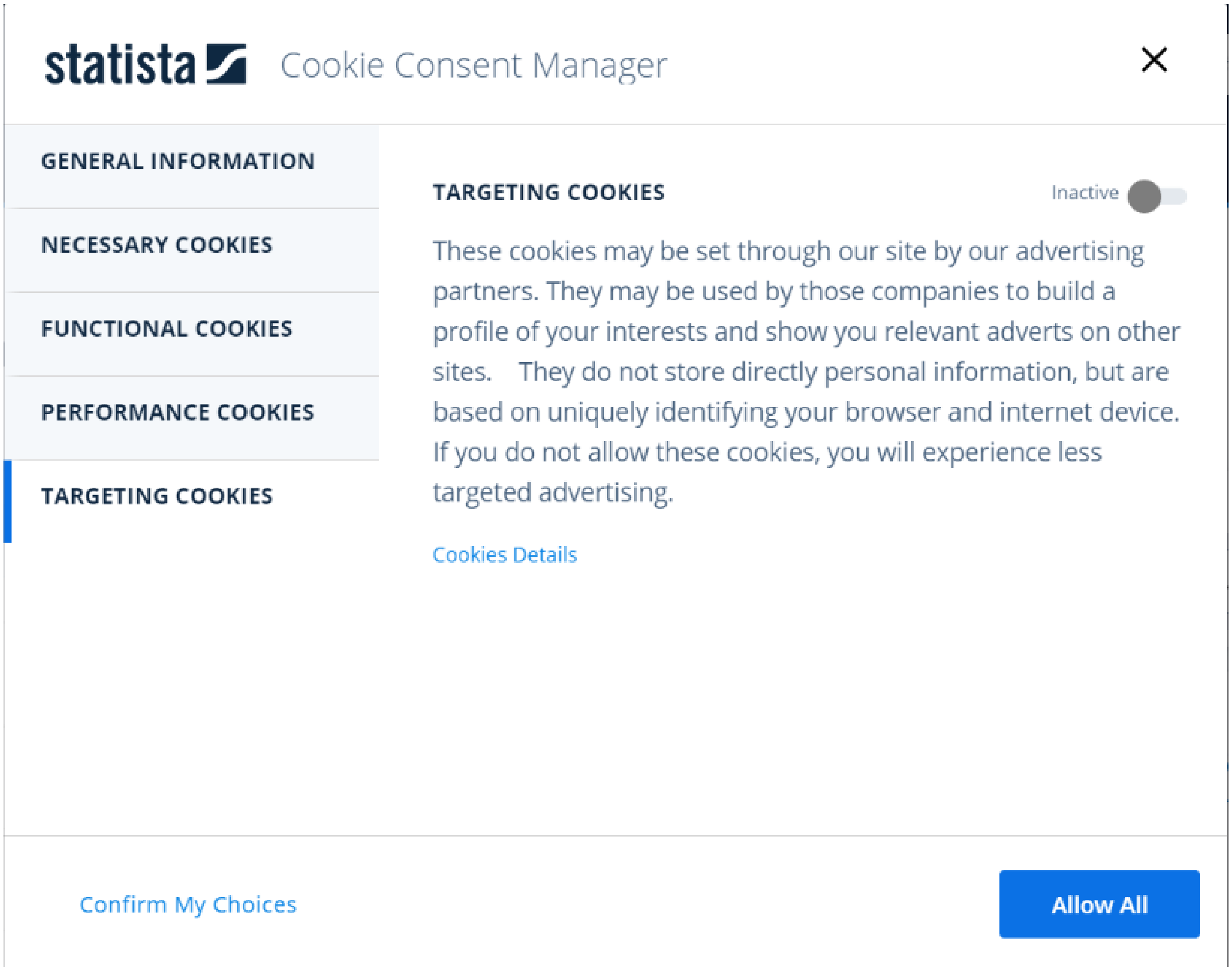
✓ Functional cookies

□ Statistics

□ Marketing

Figure 4.1 A simple option

www.manaraa.com



TARGETING COOKIES

These cookies may be set through our site by our advertising partners. They may be used by those companies to build a profile of your interests and show you relevant adverts on other sites. They do not store directly personal information, but are based on uniquely identifying your browser and internet device. If you do not allow these cookies, you will experience less targeted advertising.

Figure 4.2 Prominent ”Allow All” option

In Figure 4.1, one can see how simple it is to provide an option to the users. In case the user is wanting to see targeted advertisements, they can choose to opt-*in*.

المنارة للاستشارات
www.manaraa.com

4.2 Autonomy - Let People Choose

I propose allowing individual Internet users to control their data; insofar that a) the data being sold is clearly categorized (in that only specific data, like motor vehicle information, is required, as opposed to the full metadata of a person's life) and b) the users are made privy to how it will be used. Like opt-in over opt-out, this method will place the user's consent at a higher value than it is currently at.

I say "value" in the general idea of importance in an individual's mind of their privacy. If, for example, users start associating three minutes of their privacy with 5 US dollars, that will alter – and reduce – the perceived value of their personal data (Bataineh et al., 2020). There seems to be no accurate way to qualitatively measure the value of this privacy, but consider a hypothetical scenario: one night, an individual is faced with the dilemma of putting food on the plate. But this individual does not have access to liquid cash, so that some food may be purchased. By some mechanism, the individual is able to obtain some payment in return for sharing some personal data, or a similar aspect of one's private information for a quick meal. The perception of the individual's privacy thus changes from being of innate value to something that can provide a quick buck in a pinch (Yu et al., 2020). A side effect of such changes in perception would be that the idea of the value of the individual's privacy could become relative to the market rate of personal data.

My earlier point stands: instead of complicating these policies, let the users decide what they want to do. If a few extra dollars will help some households, so be it. But I believe privacy is a valuable right, not a luxury to be traded about. Marketing some policies like they're the perfect solution is a lazy attempt at convincing the users otherwise (Pollach, 2005).

In jurisdictions like the European Union and California, consumers now have received a legal right to port their personal data from company to company (O'Connor et al., 2020). This new wave of being able to switch services has spurred the emergence of personal data brokers. Research has shown that there is a constant struggle between data brokers and content providers to obtain the best quality user data for the best price point (Haberer et al., 2020). Models that

المنارة للاستشارات

www.manaraa.com

have arisen from contemporary research suggest that the users are losing the leverage in this struggle. In order to restore some form of economic equilibrium it has become necessary to consider letting users sell their own data (Bataineh et al., 2020).

4.3 Transparency in Design

I have found that there are also subtle but significant factors in the design structures of relevant websites. Note carefully the design choices on this cookie consent manager in Figure 3.2. The most important design choice here is a very understated distinction between the two main options at the bottom of the window. The option to “Confirm My Choices” is a dull option with no defining characteristics whatsoever, on the bottom left of the window. It’s not even a button. In stark contrast, the “Allow All” option is a rather loud button on the bottom right of the window (the typical position of most confirmatory options like “submit”, “accept”, “confirm” is the bottom right). Unsuspecting users can easily miss the distinction (Soe et al., 2020), and click the easiest button they can see (again, “Allow All” is the only button on the page), allowing full usage of all cookies on that website (Matte et al., 2020; Bauer et al., 2021). This is one of the reasons why the design principles of these policy windows should be considered more seriously.

From the previous examples regarding the cookie policy window, it is clear that most companies do not find it a worthy venture to clarify to the users of the website what exactly it is that they’re agreeing to. If the “Allow All Cookies” option gets a very visible, accessible button, so should “Save My Choices.” In fact, individuals who rely on alternative ways of technological access for accessibility purposes will not even interact with the “Save My Choices” option unless it is highlighted (Graßl et al., 2021). By default, the next logical step would be to hit the clear button on the bottom right, and proceed naturally. This also needs to be reexamined. I propose adding sections regarding this very matter in the current editions of the Accessibility Guidelines (as seen here: https://developer.mozilla.org/en-US/docs/Web/Accessibility). The European counterpart for privacy laws and regulation, the GDPR, follows a version of the 7 Principles of

المنارة للاستشارات
www.manaraa.com

Privacy by Design (Cavoukian, 2010). My proposal highly favors a set of principles based on similar values and objectives as these 7 principles, which are as follows:

1. Proactivity and Prevention
2. Privacy as the Default
3. Privacy Embedded into the Design
4. Full Functionality – Positive-Sum
5. End-to-End Security
6. Visibility and Transparency
7. Respect for Privacy

For this particular framework, I'd like to focus on the first, second, and third principles in particular. These principles have garnered thorough support from the GDPR (Nouwens et al., 2020); the first principle, Proactivity and Prevention, implies that mitigation of privacy issues be prioritized over remediation of privacy issues. By following the principle, the institution makes a commitment to adhere to the privacy standards of the GDPR. The second principle mandates that the data of the users must be protected by default. There should be no way that the user's data is affected without their knowledge, and individuals need not take action to ensure safety of their data. This kind of a value system, I think, is lacking in the West. When I say value system, I mean a general inclination towards the importance of protecting personal data, and not the monetary kind of value. The third principle is relevant to what was discussed in this section. It mandates that the functionality of systems should not interfere with the privacy protection measures already in place. In the proposal, the idea of incorporating interface design guidelines by piggybacking this third principle is put forth. UI design must include components of similar aesthetic impact – so that users can perceive them similarly – for links and buttons with similar objectives (Soe et al., 2020; Palmer, 2005; Matte et al., 2020). Further analysis should lead to the conception of the groundwork for such UI guidelines.

المنارة للاستشارات

www.manaraa.com

CHAPTER 5. Summary and Conclusion

Companies have cleverly capitalized on the slowly decreasing attention span of Internet users by displaying important notices and policy updates in windows/dialog boxes that can be dismissed easily, and lengthy, wordy EULAs. Even in real life, sufficient probable cause is required in legal systems to produce search warrants for vehicles and property. If that's the amount of convincing required for a person's private physical property to be scrutinized, then it's important to ask why companies aren't following a similar decorum. By way of tactics like employing more prominent design components in favor of tracking technologies, users are easily led to believe in a skewed version of the reality. I believe that the law should strive to strengthen the individual's rights, which include privacy.

Legislation that safeguards users from being tricked into giving up their personal data is important and necessary. Contemporary studies have shown promising research in the realm of ethical design principles; the framework proposed in this paper evaluates the three cores of the matter: opt-in architecture in cookie banners, autonomy over one's personal data, and transparency in design. Given the development of studies taking place in the realm of personal data governance, it is my hope that this kind of research brings about awareness that will improve the way we view privacy now. This dissertation aims at providing a starting point for such an endeavor.

المنارة للاستشارات
www.manaraa.com

BIBLIOGRAPHY

Almgren, R. and Skobelev, D. (2020). Evolution of technology and technology governance. *Journal of Open Innovation: Technology, Market, and Complexity*, 6(2):22.

Athique, A. (2020). Integrated commodities in the digital economy. *Media, Culture & Society*, 42(4):554–570.

Bataineh, A. S., Mizouni, R., Bentahar, J., and El Barachi, M. (2020). Toward monetizing personal data: A two-sided market analysis. *Future Generation Computer Systems*, 111:435–459.

Bauer, J. A. N. M., Bergstrøm, R. E. G. I. T. Z. E., and Foss-madsen, R. U. N. E. (2021). Are you sure, you want a cookie? – The effects of choice architecture on users' decisions about sharing private online data. *Computers in Human Behavior*, page 106729.

Bellentani, T. M. (2020). The impact of Cookie Consent Notices on user's privacy concerns : An empirical analysis.

Bornschein, R., Schmidt, L., and Maier, E. (2020). The Effect of Consumers' Perceived Power and Risk in Digital Information Privacy: The Example of Cookie Notices. *Journal of Public Policy & Marketing*, 39(2):135–154.

Carman, A. (2020). Instagram redesigns its home screen for the first time in years, adding Reels and Shop tabs. https://www.theverge.com/2020/11/12/21561099/instagram-reels-shopping-home-screen-tab-update.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. A foreword by Ann Cavoukian, Ph.D. *Identity in the Information Society*, 3(2):247–251.

Davenport, T. H., Harris, J. G., De Long, D. W., and Jacobson, A. L. (2001). Data to Knowledge to Results: Building an Analytic Capability. *California Management Review*, 43(2):117–138.

DeCew, J. W. (2018). *In Pursuit of Privacy*. Cornell University Press.

Doss, A. F. (2020). *Cyber Privacy: Who Has Your Data and Why You Should Care*. BenBella Books.

Flanagan, M., Howe, D. C., and Nissenbaum, H. (2008). Embodying Values in Technology: Theory and Practice. In van den Hoven, J. and Weckert, J., editors, *Information Technology and Moral Philosophy*, Cambridge Studies in Philosophy and Public Policy, pages 322–353. Cambridge University Press, Cambridge.

المنارة للاستشارات

www.manaraa.com

Floridi, L. (2014). Open Data, Data Protection, and Group Privacy. *Philosophy & Technology*, 27(1):1–3.

Gavison, R. E. (2011). Privacy: Legal Aspects. SSRN Scholarly Paper ID 1885008, Social Science Research Network, Rochester, NY.

Graßl, P., Schraffenberger, H., Borgesius, F. Z., and Buijzen, M. (2021). Dark and Bright Patterns in Cookie Consent Requests. *Journal of Digital Social Research*, 3(1):1–38.

Haberer, B., Kraemer, J., and Schnurr, D. (2020). Standing on the Shoulders of Web Giants: The Economic Effects of Personal Data Brokers. SSRN Scholarly Paper ID 3141946, Social Science Research Network, Rochester, NY.

Handayani, R. C., Purwandari, B., Solichah, I., and Prima, P. (2018). The Impact of Instagram ”Call-to-Action” Buttons on Customers' Impulse Buying. In *Proceedings of the 2nd International Conference on Business and Information Management*, ICBIM '18, pages 50–56, New York, NY, USA. Association for Computing Machinery.

Liu, M. and Yang, X. (2020). On the Role of “Muscle Memory” in Interaction Design. In Di Bucchianico, G., Shin, C. S., Shim, S., Fukuda, S., Montagna, G., and Carvalho, C., editors, *Advances in Industrial Design*, Advances in Intelligent Systems and Computing, pages 634–640, Cham. Springer International Publishing.

Machuletz, D. and Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(2):481–498.

Matte, C., Bielova, N., and Santos, C. (2020). Do Cookie Banners Respect my Choice? : Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 791–809.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *ACM SIGCAS Computers and Society*, 27(3):27–32.

Moore, A. D. (2003). Privacy: Its Meaning and Value. SSRN Scholarly Paper ID 1980880, Social Science Research Network, Rochester, NY.

Nissenbaum, H. (2004a). Privacy As Contextual Integrity. *Washington Law Review*, 79.

Nissenbaum, H. (2004b). Privacy as Contextual Integrity. *Washington Law Review*, 79(1):119.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., and Kagal, L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, CHI '20, pages 1–13, New York, NY, USA. Association for Computing Machinery.

المنارة للاستشارات
www.manaraa.com

O'Connor, S., Nurwono, R., and Birrell, E. (2020). (Un)clear and (In)conspicuous: The right to opt-out of sale under CCPA. *arXiv:2009.07884 [cs]*.

Palmer, D. E. (2005). Pop-Ups, Cookies, and Spam: Toward a Deeper Analysis of the Ethical Significance of Internet Marketing Practices. *Journal of Business Ethics*, 58(1/3):271–280.

Papadogiannakis, E., Papadopoulos, P., Kourtellis, N., and Markatos, E. P. (2021). User Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users. *arXiv:2102.08779 [cs]*.

Pollach, I. (2005). A Typology of Communicative Strategies in Online Privacy Policies: Ethics, Power and Informed Consent. *Journal of Business Ethics*, 62(3):221.

Smith, H. (1994). *Managing Privacy: Information Technology and Corporate America*. University of North Carolina Press.

Smith, H. and Dinev, T. (2011). Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35:989–1015.

Soe, T. H., Nordberg, O. E., Guribye, F., and Slavkovik, M. (2020). Circumvention by design – dark patterns in cookie consents for online news outlets. *arXiv:2006.13985 [cs]*.

Solove, D. J. (2004). The Digital Person: Technology and Privacy in the Information Age. SSRN Scholarly Paper ID 2899131, Social Science Research Network, Rochester, NY.

Tavani, H. T. (2007). Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy. *Metaphilosophy*, 38(1):1–22.

Wedel, M., Bigné, E., and Zhang, J. (2020). Virtual and augmented reality: Advancing research in consumer marketing. *International Journal of Research in Marketing*, 37(3):443–465.

Yu, L., Li, H., He, W., Wang, F.-K., and Jiao, S. (2020). A meta-analysis to explore privacy cognition and information disclosure of internet users. *International Journal of Information Management*, 51:102015.

المنارة للاستشارات

www.manaraa.com