Est. 1841 | YORK ST JOHN UNIVERSITY

Clarke, James Andrew (2024) Tracking Third-Party Cookies - an empirical analysis of the current situation. Masters thesis, York St John University.

Downloaded from: http://ray.yorksj.ac.uk/id/eprint/10242/

Research at York St John (RaY) is an institutional repository. It supports the principles of open access by making the research outputs of the University available in digital form. Copyright of the items stored in RaY reside with the authors and/or other copyright owners. Users may access full text items free of charge, and may download a copy for private study or non-commercial research. For further reuse terms, see licence terms governing individual outputs. Institutional Repository Policy Statement

RaY

Research at the University of York St John

For more information please contact RaY at ray@yorksj.ac.uk

“Tracking third-party Cookies: an empirical analysis of the current situation”

James Andrew Clarke

Submitted in accordance with the requirements

For the degree of

Master of Science by Research

York St John University

School

May 2024

The candidate confirms that the work submitted is their own and the appropriate credit has been given where reference has been made to the work of others.

This copy has been supplied on the understanding that it is copyright material. Any reuse must comply with Copyright, Designs and Patents Act 1988 and any license under which this copy is released.

©2022 York St John University and James Andrew Clarke.

The right of James Andrew Clarke to be identified as Author of this work has been asserted by him accordance with Copyright, Designs and Patents Act 1988

Table of Contents

List Of Figures 5

List of Tables 5

Acknowledgements 6

Abstract 8

Abbreviations 9

Defining Terminology 10

Literature Review 11

Introduction 11

Background 12

Problem Statement 13

Research Question 13

Purpose of the Research 13

Justification 14

Methodology - Prisma 15

Hypothesis 15

1.0 Current Cookie Landscape 16

1.1 Why are there cookies? 16

1.2 Security of Cookies 17

1.3 Cookie Implementation 19

1.4 EU Cookie Law 21

1.5 Who Knows About me? 22

1.6 third-party Cookies 23

1.7 Leaking Parties 25

1.8 Mobile Devices and the Cookie Monsters 25

1.9 Defending against Fingerprinting? 26

1.10 Do users care? 28

2.0 End User Understanding of Cookies 29

2.1 The Cookie Disclaimer 29

30

2.2 Mobile Tracking 30

2.3 The Hacker 32

2.4 The Tracker 33

2.5	Does Tracking Protection actually work?	36
2.6	Server Cookie	37
2.7	Tracking the trackers	39
2.8	Privacy Loss	40
2.9	Web Privacy attacks	41
2.10	Identifiers	42
2.11	The Web never forgets	43
3.0	Current Cookie Laws and Regulation Including Their Failures	44
3.1	What is being done to stop Cookie information being shared	44
3.2	European Union's Say	45
3.3	What has to be done with Privacy?	47
3.4	Cookies Security Failures	48
3.5	Privacy analysis	50
3.6	Challenges in supporting Privacy	52
3.7	third-party Tracking	53
3.8	Tech Platforms as Privacy Regulators	54
4.0	Potential Improvements In The Use Cookies	55
4.1	The Blockers	55
4.2	Hidden Web	56
4.3	OpenWPM could be the answer	57
4.4	The Cracked Cookie Jar	58
4.5	User Agent	59
4.6	Privacy Audit	59
4.7	The Cloud	61
4.8	Blocking	62
Analysis		63
Conclusion		64
Future Research		65
References		69

LIST OF FIGURES

Figure 1: Whether the participants would leave the website on seeing a cookie disclaimer. (Gerber, N. et al, 2018). 30

Figure 2: Percentage of URLs that contain third-party (TP) and third-party tracker (TPT) cookies. 36

Figure 3: Top 20 organizations by combined tracker's reach. 40

Figure 4: Dropbox UI of the victim's account during the Unexpired Email Change Attack(Paverd, A. et al, 2022). 50

Figure 5: Average decrease in tracking with blocking tools. (Mitchell, J.C et al., 2012). 63

Figure 6: The Ford website in the EU with a link to another page for the user to manage their cookie preferences. 66

Figure 7: The EU sites cookie preference settings shows 4 separate types of cookies and fully explains their use and consequences of inclusion. 67

Figure 8: Example of the same companies US sites cookie page with the limited selections available to the user. 68

LIST OF TABLES

Table 1: The focus is on the implementation of cookies and the analysis of their impact on the data collected from users. 18

Table 2: Websites showing the Cookie Bar then refreshing the page once user consent is given. 21

Table 3: Availability of cookie consent notices in the top 500 websites by country, pre- (January 2018) and post-GDPR (after May 25, 2018) 45

ACKNOWLEDGEMENTS

This thesis would not have been easy without the support of many Individuals in my life.

Aminu Usman, Associate Head of Computer and Data Science and Supervisor at York St John University

Mike O'dea Senior Lecturer and Supervisor at York St John University

I want to thank my supervisors and mentors, Aminu Usman and Mike O'dea, for their knowledge, time, and patience throughout the duration of my MRes. I am so lucky and thankful to have such wonderful people guiding my MRes student experience. This is just one of the many roles that you fill at the University. I appreciate your endless amounts of patience. Whether it be meeting in different time zones or with short notice, you always were available for me and provided invaluable support. I appreciate you both for encouraging me to take a risk and create a study involving the privacy of cookies. With your guidance, you helped me to conduct this study, to ask tough questions, and to fulfill my desire to research cybersecurity. I would not have been able to successfully complete my MRes without your support.

Mom and Dad

I am incredibly grateful for my parents, Helen, and Warren Clarke, who have supported me throughout my life and especially during this process. Being In a different country than my parents for most of my university life was not without its difficulties. The encouragement and support they gave me felt like they were right by my side. They always have supported all my dreams, encouraging me to complete my MRes, and cheered me on from the sidelines. It is difficult to fully articulate my gratitude and appreciation for my parents, who have always encouraged me to push myself to go higher than I think.

Matthew

I want to thank my older brother Matthew for your friendship. It has not been easy being away from you for so long. You continue to remind me that I am capable of doing difficult things out of my comfort zone, and you have always pushed me to be a better student.

Sam

An incredibly special thanks to my partner, Sam. As you have been working on your MBA, you have kept me on track and pushed me with our many study sessions at the library. The constructive criticism you have given me on this work has helped immensely. I am lucky to have met such an intelligent person that always encourages me to be the best version of myself.

I2I Orange

I am grateful to be part of such an incredible soccer team. I never dreamed that I would have found some of my closest friends; they have always believed in me since the beginning of my university journey in 2018 and continue to encourage me to this day. I am so thankful to have been a part of the amazing journey that is sadly ending but am lucky that I continue the friendships. To the Orange Team, I cannot thank you enough.

Chris and Nelly; Coaches at i2i International Soccer Academy

Lastly, I want to highlight my soccer coaches, Coach Chris and Coach Nelly during my soccer and University journey. You gave me the best advice, and the skills I practice on the field translate into my academics and my daily life. It is hard to put into words the difference you made to my life during my time in York, and I must mention the laughs we had along the way. Thank you!

ABSTRACT

Through the act of browsing, “users,” or the individuals who participate in internet searches, develop their digital footprint cookies. Essentially, cookies are trackers stored on a user’s computer by a website or application. The trackers collect data that provides users with a more relevant internet experience. While cookies have proven to enhance user experiences on the internet, they also encompass a range of concerns over privacy and user safety. Notably, the way cookies both store and track PII (Personal Identifiable Information) without user’s consent is a significant concern. When users enter a webpage, there is an options box that prompts them to accept or reject cookies. It is unclear how transparent this process actually is, as these sites may still store user’s personal information, even after they have elected to “reject” cookies. **Discussion:** Therefore, the primary aim of this thesis is to understand how cookies affect the user and determine what kind of technologies or strategies can be implemented to ensure the user has a better network experience while guaranteeing that their information is secure. This will be done by researching existing published research on various aspects of cookies to understand how cookies are typically used. The detail of the methodology is discussed on page 14. **Conclusion**: Ultimately, it is essential that users know how to utilize cookies sensibly, it is vital to share the user’s cookie policy and protect privacy as much as possible. The main finding was that there was a gap in existing research as no articles tried to discover which 2 main sets of regulations, in the EU or US, was being implemented more successfully. The information required to do this simple analysis, such as the regional location of a site and user, is typically available but was not published in the research material.

ABBREVIATIONS

HTTP	**HyperText Transfer Protocol**
Etags	**Entity Tag**
PII	**Personal Information**
GDPR	**General Data Protection Regulation**
MAC	**Media Access Control**
Hash	**Hashtag On a computer**
PKI	**Public Key Infrastructure**
CCPA	**California Consumer Privacy Act**
CSRF	**Cross Site Request Forgery**
IDP	**Identity Provider**
AJAX	**Web Development Techniques**
MFA	**Multi Factor Authentication**
FTC	**Federal Trade Commission**
SSO	**Single Sign-on**
IDP	**Identity Provider**
HSTS	**HTTP Strict Transport Security**

DEFINING TERMINOLOGY

Cookie Sniff, a type of network attack on cookies to find more about a user's search history

GET method, HTTP method that is requesting information from a specified resource which remains in the browser's history

Federated, allows users to access multiple apps and domains using a single set of credentials

Public Key Infrastructure, a key management system that uses hierarchical digital certificates to provide authentication, and public keys to provide encryption

ePrivacy Directive, an important legal instrument for privacy in the digital age, and more specifically the confidentiality of communications and the rules regarding tracking and monitoring

DNS Blacklist, is a spam blocking lists

LITERATURE REVIEW

INTRODUCTION

Internet users value their privacy, their ability to search, and to freely use internet resources, but because of the productiveness and confusion surrounding cookie downloading, it is unclear whether or not users truly have the privacy they think. While users may acknowledge that their activity on the internet can be tracked; unbeknown to most users, cookies are the primary mechanism used to track their internet activity. Cookies threaten user privacy by collecting personal information such as the user's name, email address, location, and purchasing history. As the user maintains and builds their presence on the internet, they will inevitably have to accept and reject cookies, and these cookies will continue to collect their personal information, creating an internet identity for each user.

There are two types of cookies, third and first party, that shape user experiences on the internet. Third-party cookies differ from first party cookies in two ways. Mainly, third-party cookies are not sent through the response to a page request; rather, they occur in images, ads or scripts hosted on a first party website by a third-party server. The other way third-party cookies differ from first party cookies is that they can be used across different websites and internet sessions instead of a single visit (Heyman, R., 2011.). Third-party cookies ensure that PII can be stored in the website domains and even shared across different ones. Third-party cookies, which are stored on a website by someone other than the user, come at a significant privacy cost. These companies that have collected personal information can create detailed profiles about users, which can be viewed as infringing on their privacy rights. In recent years, civil society organizations and policymakers have drawn attention to how third parties can track a user's browsing activities across the web. This tracking imposes a level of vulnerability onto the user. While user's can prevent their information from being stored and tracked in multiple ways, so long

as web companies lack transparency, it is unclear how effective these security-ensuring actions actually are.

BACKGROUND

With technology's rapid adoption, growth, and influence in every aspect of our lives, users must be able to protect themselves from unnecessary and harmful data collection. Cookies threaten user safety across all technological platforms; they are text files made up of tiny pieces of data that are used to identify the user's computer by how they use the network. More specifically, third-party cookies are used by websites to identify specific users and improve the users web browsing experience. For example, cookie collection might send targeted ads which are beneficial to both the user and the company, and if the company understands what the user's wants and needs are, the more likely a customer will respond to advertising. When the user response is engaged with the brand or company, then they would purchase the product which will benefit the company. Cookies collect data through a multi-step process. Cookies are tracking codes that are placed on a web user's computer after being generated by a website other than the one the user is on. When the web user visits other websites, their information will continue to be stored and tracked across different browsers. Lastly, this information that is part of the third-party will send it to the third-party that originally created the cookie, such as an advertiser. The server creates the data stored in a cookie when the user secures an internet connection. Following this, the data derived from the internet connection is labeled with a random ID that is individual to the user and the computer. The ability for cookies to identify and alter internet experiences based on individual preferences highlights the issue of trust and transparency, a fight over privacy between users and company sites. The issue of privacy means that laws like GDPR (General Data Protection Regulation) needed to be created by the EU to protect data protection and privacy in the EU and European Economic Area. GDPR seeks to prevent the creation of user profiles and regulates the

processing of personal data by an individual, a company, or an organization of personal data (Weippl, E et al., 2019.). GDPR is just one law in the EU that seeks to regulate the ever-expanding privacy issues that are emerging from cookies and cookie data collection. However, it is evident that new types of laws are needed to regulate privacy issues throughout the web and to protect users, especially from third-party cookies and domains.

PROBLEM STATEMENT

This study evaluates the relationship users have with trust and technology, to raise awareness about the issue of trust and transparency between users and companies on the web.

RESEARCH QUESTION

My research question is broadly intended to ask, what do user's need to know about third-party cookies? Why do they not already know this information? Are laws and regulations effective at curbing third-party cookie abuse? In my research I incorporate information from social, economic, and legal realms, as part of a broader systemic inquiry into how powerful stakeholders can control user's internet experiences through cookies.

PURPOSE OF THE RESEARCH

As online activities continue to grow and evolve, understanding how cookies impact users is essential. The study aims to understand cookies' impact and find strategies for secure, improved user experience. This study acknowledges the dual nature of cookies, highlighting both their benefit to user experience and the potential risks they pose.

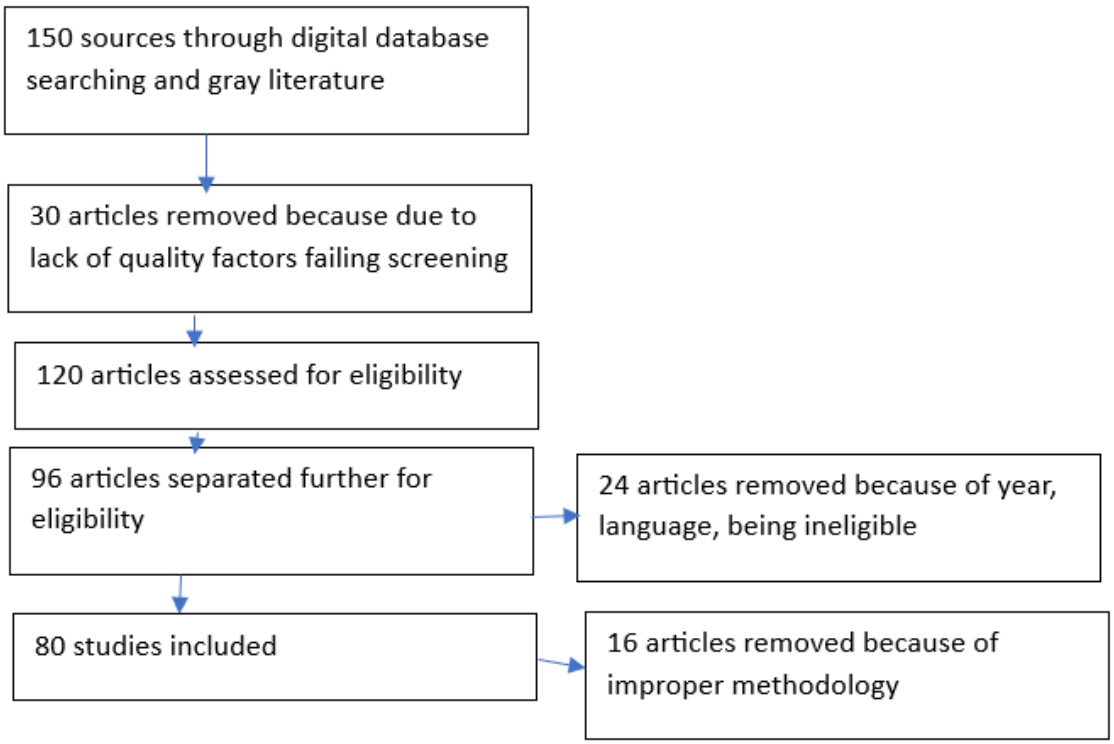
JUSTIFICATION

Despite the negativity that third-party cookies get, user's experience many benefits from them. Cookies make the internet more convenient for users. While using cookies, users can take advantage of the pre-filled out address information when they are making purchases. This makes online purchasing much faster and more simplistic. Websites can also get user's locations to see the most relevant information in their area. For example, companies can identify where users are located and give suggestions for activities or food. Personalized information is another massive benefit users receive from cookies. For example, users may get videos on their YouTube feed related to their browsing history and interests. This allows users to achieve greater exposure to topics that they are already interested in, and to new, related topics. Third-party cookies also send relevant ads to users, providing them with advertising content suitable to their interests. This targeted advertising will inevitably expand user markets and create more revenue for businesses.

While third-party cookies provide users a range of benefits, they also are a significant source of discontent. Users have developed distrust because they feel as though their privacy is being confiscated. Cookies allow the user to be tracked by every website they visit, and each website collects a great deal of information about each user, then passes it on to other websites. Users also fear for their personal and physical security as the software allows outside parties to access personal information like addresses, names, and even credit card and bank account numbers. Specifically, because it may be difficult for users to adequately "accept" or

"reject" cookies on all browsers they encounter and because software companies are monetarily incentivized by storing more data, user's private information could be compromised in numerous ways, and this might be difficult for them to track.

METHODOLOGY - PRISMA



HYPOTHESIS

If there are more laws and regulations about third-party cookies that incorporate contemporary knowledge and wording regarding user safety and privacy, user's will be more likely to elect to "reject" cookies when they load their browsers, because more laws that include comprehensive

regulations equate to better systems wherein the user has an established understanding of the privacy implications of accepting third-party cookies.

1.0 CURRENT COOKIE LANDSCAPE

1.1 WHY ARE THERE COOKIES?

Cookies make it easy to build stateful web applications which can save a user's session data. They are not necessarily essential to achieve that purpose, in order to accomplish the same thing, a server can embed stateful info in URLs, use forbidden fields in HTML forms, or use the clients IP address. However, these approaches do have many issues such as privacy and security errors. For example, IP addresses are an unreliable way to identify a user or computer, rather than being contained within the user access information, that the user can access info that the servers give back to the user. If a user clicks on a back button in the browser, the user's information would roll back to what was on the page before. For a shopping application, this behavior would have the effect of removing items from the shopping basket. However, both approaches lend themselves to not cooperating. Users can easily capture the text of the URL or form fields, edit it, and resubmit the information to the server, with unpredictable results. Lastly, embedding state information in URLs is very unfriendly to caches, and web caches are considered valuable for reducing network traffic and, thereby, congestion. URs can only access a single file while cookies can access multiple files.

In contrast, a cookie that is stored on a user’s computer is the same as the path by which the user’s computer connects to a domain such as www.example.com. The cookie contract specifies that the user’s computer returns its cookie to www.example.com when they visit it again. Regardless of what their IP address is on a single-user computer like a PC, the cookie can identify the collection of all users of the computer. On a multi-user computer, the cookie identifies the user of a particular account. The user's

Identification does not necessarily mean that www.example.com somehow knows their name, address, or other personal information. Unless they explicitly provide personal information, all that www.example.com can do is assemble a list of URLs on its site that they have visited, as identified by a cookie. Of course, if a user supplies personal information to www.example.com, perhaps to register for some service or to order merchandise, that information can be associated with the URLs they have visited. Therefore, cookies possess the ability to monitor user browsing habits and associate browsing history with a specific user. This ability of cookies to identify personal information is a significant issue.

1.2 SECURITY OF COOKIES

Users experience three main security threats with web cookies. These threats are confidentiality of the user, monitoring the user activities, and the malicious embedding tags in cookies to introduce embedded code (Mitchell, C. et al, 2002). In the paper "Enhancing the security of cookies" written by Vorapranee Khu-smith and Chris Mitchell, the primary research aim is to address confidentiality and malicious embedding of tags. The research did not encompass monitoring cookie activities because the researchers felt that there were many tools that already existed and were designed specifically to monitor the activity of cookies rather than user activities. The confidentiality of the user is two-old; it includes both transmitting their information from their web browser to the web server or their information stored on their client, including a public shared client. The integrity of a cookie even has the ability to be compromised in such a way to prevent the true authorized user from having access to the web server by hijacking their profile and possibly embedding tags to malicious code.

There are good protection requirements out there for users: The first two are very generic and used in conjunction with each other as well as with a third type that had two vastly different approaches, which is where they wanted the paper to discuss in more detail. The two basic methods are to use Secure

Channels, which protects users' data in cookies during transmission between their web browser and the web server, but not protecting their data stored on a client (Mitchell, C. et al, 2002). The other basic method is to use Access Control on the user's client, which prevents the users' cookies being read externally by others.

The main discussion for the paper was between the two main methods of using cryptographic protection. Both types introduce kinds of cookies like Name, Life, and Key, but simply put it is basically where encryption utilizes keys and the Seal containing a MAC or a signed hash of the other cookies (Mitchell, C. et al, 2002). They might require a web browser and possibly even software changes by the user. The first method is to use server managed cookie encryption, which can be site specific, but they would reference the more generic type that encrypts all sites or applications called the "Secure-Cookie." This is shown in table 1, where each cookie name in that domain is not secure. These do require a cookie issuing server which the web browser sends to the web server and addresses the two remaining earlier cited security requirements of confidentiality and malicious but now introduced a new requirement to prevent replay type security attacks. This is where the second method of user managed cookie encryption (Mitchell, C. et al, 2002). This will require a special web browser and software installed on the client. This stores the cryptographic key on the client which could be a security hazard, so key management software is used. This method also has two approaches, symmetric and asymmetric cryptographic protection that both have the user request cookie encryption to the web server which triggers the encryption key protocol to be established. The user authenticates themselves even on a public client using secure channels on its transmission including a MAC and time stamp to prevent replay attacks. Asymmetric also includes the use of certificates with the key and requires Public Key Infrastructure (PKI) for certificate management. The protocols for both the symmetric and asymmetric user managed cookie encryption were also discussed**.** Simply that cookies pose a security threat and that there are four security requirements of user

authorization, confidentiality, integrity and replay protection. The last requirement of replay protection is only met by user managed cookie encryption (Mitchell, C. et al, 2002).

Domain	Flag	Path	Cookie_Name	Cookie_Value	Secure	Date
acme.com	True	/	Name_cookie	Alice	False	12/31/2000
⋮	⋮	⋮	⋮	⋮	⋮	⋮
acme.com	True	/	Life_cookie	12/31/99	False	12/31/2000
acme.com	True	/	Pswd_cookie	Hashed password	False	12/31/2000
acme.com	True	/	Key_cookie	Encrypted key	False	12/31/2000
acme.com	True	/	Seal_cookie	Signed Message Digest of MAC	False	12/31/2000

Table 1: The focus is on the implementation of cookies and the analysis of their impact on the data collected from users. (Mitchell, C. et al, 2002).

1.3 COOKIE IMPLEMENTATION

Cookie implementation is helping the website remember information about each user's visit, which can make it easier to visit the site again and make the site more useful to the user. Focusing on the implementation of cookies and the analysis of their impact on the data collected from users. Each type of cookie is described by their functionality and also the privacy management software that is used in processing. Two important regulations concerning the protection of user privacy have been implemented in the US and the EU. The EU uses the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) is what helps regulate data protections in the United States (Krstovic, S et al., 2022). While these two new regulations cover different regions and countries along with vast numbers of diversified users, analyzing how they compare and differ can offer insight into the state of data security.

Because these regulations are institutionalized within different regions and government capacities, they have a different impact with regards to cookies and user privacy.

The two regulations are mostly similar but have some fundamental implementation principles that are different. These data protection principles such as the Lawfulness, fairness and transparency can cause significant gaps between the two regulations that mean online safety and privacy are variable for user's depending on where they are geographically located. These gaps and challenges are with processing technological capabilities that arise from the introduction of multiple data protection principles (Krstovic, S et al., 2022).

The technological challenges that the principal's differences reference arise from three distinct aspects of usership. The first, is from a user perspective, then from the technology viewpoint where it must be in tune with new monitoring techniques. The third aspect relates to privacy policy, and how it should connect technology and users and maintain a level of transparency. After the GDPR and the CCPA were introduced, users had greater confidence that their data was safe and protected by laws. Online Business owners had a larger problem with secure storage and knowing when to revise databases to stay updated with the correct online laws. (Krstovic, S et al., 2022). The GDPR and CCPA have led company data controllers to follow strict approaches when selecting data processing technologies. Companies that build their reputation for compliance with the law have an opportunity to gain a competitive advantage in the data world The GDPR and CCPA have already had an impact on data protection technology development companies that are in the global market to ensure that their data, products, and services comply with legal requirements and sell their products to the companies that have built their reputation on compliance with the law.

From a user perspective, the fundamental issue of a cookie disclaimer is requiring the user sign up for their data protection as they enter a site. However, many users do not understand that these

disclaimers serve to protect their privacy and security. Research emphasizes the importance of websites providing clear information about cookies to users. In Krstovic et al, media sites in the US and EU were examined to see what cookie policies exist at each site and how that information is presented to a site user. The study investigated multiple websites to answer five fundamental questions. These questions were as follows: Does the site have a cookie notification? Does the site have a privacy policy? Does the site implement privacy management software? Is the site functional if cookies are disabled? Is the cookie policy link separate from the privacy policy link on the homepage? It was found that each site is attempting to conform to the regulations that are pervasive to their site's users and their regional areas. It was also found that these cites often do not comply with the other regions' regulations, meaning cookie policies are regionally situated. Krstovic et al, provides some proposals and critical opinions on safety and potential directions for future development (Krstovic, S et al., 2022). One of these proposals calls for browser developers to implement a simple chatbots or browser extension that extracts a site's cookie policy. t. The chat box or browser will then present the findings to the average web user in a straightforward way so that they can identify the security characteristics of the site. Doing this will help the user to gain full transparency of each site's policies, which will then help them to decide whether to utilize that site or to find a different one.

1.4 EU COOKIE LAW

The EU is now one step ahead of all the other countries as they have made the GDPR law. The continuous collection of personal information from users makes them feel uneasy about their privacy. The EU introduced a first set of regulations on the use of online tracking technology (Marco, M. et al, 2019). This is aimed to make online trackers very explicit to raise awareness of privacy among users. The EU Directive mandates websites to use informed consent meaning adequate information, voluntaries and competence given to the user before deploying cookies. Since 2013, the ePrivacy Directive has been

mandatory, and each EU member State transposed it in national Legislation. Since then, most European sites embed a HTTP cookie (Cookie Bar) that is then stored on a user's computer so when they revisit the website, a user's browser sends information back to the site, which makes this the most visible effect of the regulation. There is also a large-scale measurement campaign to check the current effect of the EU cookie directive on user safety. To complete this measurement campaign, a CookieCheck that exchanges the cookie between a user's computer and the network server, the server then reads the ID and knows what information to serve to the user (Marco, M. et al, 2019). Resulting from the cookie check that was conducted in the year 2019, it was found that over 49 percent of websites do not show a cookie banner, and this is significant because it means that the EU directive is ineffective in protecting user privacy and implementing regulations. As shown in Table 2 below, 3 major countries in the EU and if a cookie banner is shown.

Country	Banner		No Banner	
	No Refresh	Refresh	No Cookie	But Cookies
France	69	2	11	18
Germany	31	0	18	51
Italy	53	14	15	18

TABLE 2: Websites showing the Cookie Bar then refreshing the page once user consent is given (Marco, M. et al, 2019).

1.5 WHO KNOWS ABOUT ME?

The task of protecting users is more difficult than ever because of the negative attitude towards personal information that can be leaked. Users need full understanding of the tracking and advertising industry, to make safe choices about their internet activity (Krishnamurthy, B et al., 2013). Despite the

ongoing issues of data leaks that occur on popular social media sites and the widespread acknowledgement of user vulnerability in the press, many users still do not understand that their personal information is being tracked across these sites and used by tracking companies. There have been many efforts to address individual awareness of the egregious aspects of data collection and also efforts to develop tools that make this process more simplistic for users. Researchers Krishnamurthy, B et al., found that there is a more comprehensive and efficient client tool called NoTrace awareness that can help user's gain awareness to the extent of how their personal information is being leaked. This tool can help users make better decisions about controlling their online data footprint, a user may find that a social media site they commonly use is collecting their personal data and may decide to delete their account or may not go back to that site again. NoTrace awareness empowers users with a clear overview of the availability of their personal information, allowing them to make their own decisions on feasible countermeasures for their own privacy. NoTrace supplies several measures to limit personal and sensitive information, NoTrace provides privacy protection at a lower cost without degrading page quality or causing functional breaks. NoTrace also supplies mechanisms to inspect real time content of web pages. Lastly, awareness about data leakage is provided only by NoTrace (Krishnamurthy, B et al., 2013). Using reverse engineering, NoTrace can show user's what type of leakage is going to the top 10 aggregators. The platform can even determine what percentage of a user's profile is leak able and trackable and available to trackers and hackers. It has found that one of the top 10 aggregators has the ability to collect 87 percent of user's personal information from their online profiles alone such as their bank accounts (Krishnamurthy, B et al., 2013).

1.6 THIRD-PARTY COOKIES

Data Privacy, or user integrity, has become a significant contemporary concern amongst users. Many of these privacy concerns are a reaction to the massive increase in the use of third-party cookies

during a user's browsing session (Nilsson, J., 2023). Research has shown that the prevalence of third-party cookies affects user's experiences and integrity, leading them to question their personal security when online. While measurements of consumer integrity vary from one user to the next, researcher Nilsson J., has found that it depends on a range of factors like the strength of privacy policies, trust in the organization that is collecting data, and the user's perception of fairness (Nilsson, J., 2023). The variability of individual user integrity and thought around user integrity is especially significant, as the discussion of user privacy is continuously evolving as third-party cookies become more prevalent Nilsson, J., 2023). While some consumers do not want their data to be tracked and stored at all, others express curiosity or making allowances for cookies with proper information and understanding (Nilsson, J., 2023). When determining what sort of regulations to implement for third-party cookies, it is essential to acknowledge that every user requires something different. Some users want maximal security, while others appreciate the shareability of their information from one browser to the next. The variability of user needs sets a high standard for creating laws that allow users to identify their place and then make informed decisions about accepting or rejecting cookies or installing toolkits. Even so, contemporary laws like the GDPR, although it may not completely encompass issues of integrity, is a significant step to educating user's and creating regulations that protect their safety.

Third-party cookie removal is deviated from other mega trends in the world. Users' main concern is the data collected about them has made authorities step in and take actions (Oksanen, T., 2022). Over 60 percent of adults have agreed that companies have way more control than they should over someone's sensitive information, the adults believe that the users should have more control over what websites can do with their personal information. Also, more than 50 percent of users were genuinely concerned about their online privacy data from 2019, the users believe with their digital footprint growing every time they go on the web, it causes more issues between the user and the company. In 2018 the EU General Data Protection Regulation and in the United States somewhat similar legislation California consumers act went

into effect. These both have the right of protecting the consumer's private data (Oksanen, T., 2022). Users believe these laws are a step in the right direction as the users want more power over their information, users believe more regulations will help users feel safer on the web.

1.7 LEAKING PARTIES

Third-party tracking first began in the 1960's, but it has expanded, mostly without regulation, at the expense of user security (Gardner, G.J., 2021). The original ways of tracking through HTTP cookies, adobe flash, are disappearing because. Super cookies, ETags, the Evercookie, and JavaScript fingerprinting have replaced these older models of third-party tracking, as contemporary modes of tracking. First party HTTP and HTML5 cookies respawned on sites like hulu.com through a service hosted at kissmetrics.com. Cookie respawning is the process of creating cookies from information that has previously been deleted. Regenerating the cache to mirror values, specifically ETags, ETag tracking is a problem as the technique generates tracking values even when the user blocks Flash, HTTP, and HTML5 cookies (Hoofnagle, C.J. et al, 2011). Another ETag disadvantage is it has slow load times and crashes multiple times in the same resources by having higher server load and used bandwidth. This expansion in tracking and collecting user data has occurred alongside an expanding corporate marketplace predicated on trading user data (Gardner, G.J., 2021). Wide scale data trading is especially problematic, as with big data being captured via web browsers and gathered from smartphones, the existing streams of consumer demographic and purchased data can now be painted using big data. This has been merged with behavioral analytics data to create incredibly detailed pictures of users with no clue of them knowing.

1.8 MOBILE DEVICES AND THE COOKIE MONSTERS

The rapid development of mobile phones and tablet computer usage is another threat to cookies because it is a threat to user privacy as users are being tracked on more devices. In the UK, mobile phones accounted for over 75 percent of the time spent online by users. Over 65 percent of all digital advertising spending happened on these devices in 2018 (Beauvisage, T., 2020). it is not possible to install cookies in mobile applications. In addition, for Apple smartphones, a large share of web browsing time is spent on the Safari browser, which blocks third-party cookies by default. The incompatibility between cookies and the mobile environment is a serious limitation for advertisers because it raises two types of problems: what identification technology can be used in the mobile environment to replace the cookie? How to "reconcile" computer and mobile usage to keep on tracking users from screen to screen and to create a coherent picture of them? At first glance mobile devices are not cookie friendly; the developers of mobile devices have provided a solution to the cookie (Beauvisage, T., 2020). The developers of mobile operating systems have created advertising tracking and targeting by mobile operating system developers. This mechanism makes it possible to match the information collected on a user by different advertising vendors by continuing operations from one application to another. From this mobile advertising IDs are the testimony of how cookie infrastructure serves as the main digital ads that is maintained beyond just the cookie itself.

1.9 DEFENDING AGAINST FINGERPRINTING?

There are technologies like a VPN that are marketed for their ability to enhance user privacy, but they often result in making fingerprinting easier. An example is a user agent being disguised as one of a different type (Agent spoofing) and flash blocking browser extensions allows users to prevent page

elements such as HTML object tag browser plug-ins and ads from being shown (Eckersley, P., 2010). Without vital legislation, there remains a controversial paradox as many technologies that attempt to safeguard users from fingerprinting are actually fingerprinting users. The measurements that are being done to improve user privacy that are not very effective is Flash Blocking as it is increasingly vulnerable to potential cyber-attacks, and User agent alteration as a user can manipulate the user agent on a user's monitors to test content meant for other browsers or operating systems (Eckersley, P., 2010). Researcher Eckersley found when conducting research on a small group of users having privacy in their agent strings, which are intended to identify devices requesting online content, were surprised that their purportedly privacy enhancing browsers were this vulnerable.

In the study conducted by Kristol D.M, called HTTP Cookies: Standards, Privacy, and Politics he found, an initial reaction from the advertisers for the initial setting for third-party cookies is clearly negative. users did not see the need to ask for permission before setting up cookies as they felt that asking for it would cause an issue. The public sees this and starts to become uneasy, which led to the support of techniques such as certified cookies (Kristol, D.M., 2001.). Certified cookies help users to feel more comfortable by being more secure such as HTTPS, Certified cookies should definitely be noted that disabling cookies does not completely eliminate the data being collected by third-party users as some website owners make the users accept cookies or they cannot use their website. (Kristol, D.M., 2001.). Web bugs are malicious code that is invisible to a user that is placed on websites that allow third parties to track use of web servers and collect information about the user. The information can be used to do the exact same thing and browsers that use their own ads can create profiles of any user on their sites, this is using cookies within their own domain. The good news is browsers are not as effective because it is from just one site or a few related sites. Users may not know about this but, the advertisers frequently insist they create anonymous profiles to be used to target their advertisements. Ad companies have no plan to match the profiles with personally identifiable information meaning that the companies are just using a

basic image of the user and not a detailed one. The behavior of the Ad companies is the user's greatest fear and can be confirmed within the standards of the third-party cookie process (Kristol, D.M., 2001.). The standards are usually set by the companies or by the users to create a safer web browsing experience.

1.10 DO USERS CARE?

Researcher Kristol D.M did a study [WebSideStory 2001] that showed that users reject less than 1% of cookies from over one billion views on a single browser. There are lots of reasons among users, users have never even heard about cookies, they don't know how cookies are used to track them, users know how they are being tracked but don't care enough, users don't have knowledge so they just give in and accept all of the cookies (Kristol, D.M., 2001.). Users assume the browsers storing the cookies will protect their personal information. The user might assume the government will prevent websites from misusing information that they can collect as the Privacy Act of 1974 prevents unauthorized disclosure of personal information. User concerns for online ad blocking suggest that users should be blocking ads, ad blocking should be the responsibility of the publisher and the Ad agencies. The ad blocking user penetration rate in the United States stood at just over 25% in 2020 meaning that around 73 million internet users had installed some form of ad blocking. Over time users would go towards the more responsible publishers with better ad policies as this will determine the behavior and privileges for users and computers. So far this has not happened quite yet as there needs to be more information on good ad policies, most users have claimed that on so-called good websites such as email sites, users have encountered bad Ads (Panjwani, S. et al, 2013). User preferences for and against ads are hugely complex and some users may want child friendly ads at home but not at the workplace. the ways that they vary and are complicated require unique laws to help manage all of these complexities, some may suggest that current ad blocking tools are what the user wants. An end- user browsing assistive tool which

injects a Javascript code into the users Web browsers and enables users to disable tracking on the web, and selective ad blocking, for example blocking Ads which depend on the users wants and needs. A good tool today that could be useful is AdBlock plus but less than 5% of all website users actually use this (Jaiswal, S et al., 2013). Ad block plus blocks Youtube ads, follow along video ads and banner ads. Without legislation for tracking that is informative to users, programs like ad blocks will never garner the user base that they should, even though it is an immensely helpful tool.

2.0 END USER UNDERSTANDING OF COOKIES

2.1 THE COOKIE DISCLAIMER

Since 1994 cookies have been programmed or embedded within internet browsers to improve user experience and functionality. Considering their early implementation, cookies have been universalized across the internet and have progressed to the point that includes data collection from each user. During a user's browsing experience, they will encounter a cookie disclaimer, which is a pop-up notification that asks users to either "accept" or "reject" cookies. Even though this cookie disclaimer has historically been used to provide clear, understandable, adequate information to the user regarding cookies, research shows that privacy and security notices are often ineffective in their purpose (Gerber, N. et al, 2018) (Refer to figure 1). In fact, as users are expected to make decisions about cookies, it is evident that the term "cookies" itself is confusing and misleading. Many users do not know or understand what they are, and they blindly accept or reject without ever looking into the true meaning. Many users also might not read or successfully locate the cookie disclaimer message. The cookie disclaimer is also complicated by how misleading it can be for users, whose data can still be stored and tracked across different websites even after they elect to "reject" cookies when they receive the disclaimer. This process of third-party data collection and sharing is not apparent or presented within

the disclaimer because it does not differentiate between first and third-party cookies. This fact means that users do not understand the extent that they are being tracked across multiple browsers or internet sessions. The data in figure 1 proves that cookie disclaimers are ineffective for users, as 58 percent of users claimed that they would not leave a browsing page if they saw a cookie disclaimer (Gerber, N. et al, 2018). These users ultimately have decided not to leave the page because they may not understand the implications of cookie downloading and the ways in which their personal data could be subject to tracking. Additionally, 23 percent of users responded with indecision, unsure of whether or not they would leave a page with a cookie disclaimer (as shown in Figure 1). Their ambivalence reflects the complexity of cookies, and the inability of the everyday user to understand what cookies are and how they are affected by them.

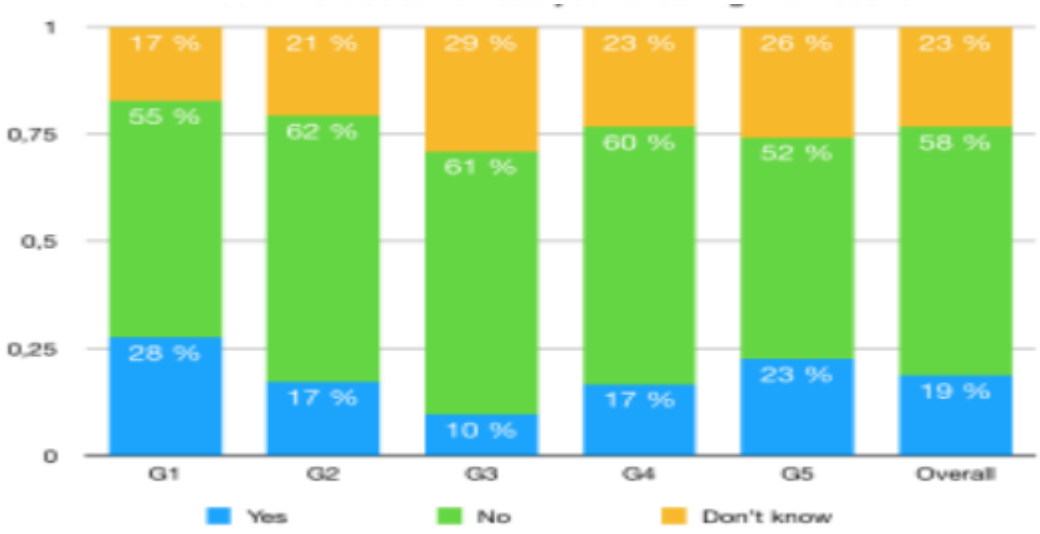


FIGURE 1: WHETHER THE PARTICIPANTS WOULD LEAVE THE WEBSITE ON SEEING A COOKIE DISCLAIMER. (GERBER, N. ET AL, 2018).

2.2 MOBILE TRACKING

There is a big talk about privacy in mobile phones, and mobile tracking. There is simply no operating support system, which is a set of programs that helps a communications service provider monitor, control, and manage a computer or telephone network on mobile phones that defines third-party cookies (Wetherall, D. et al, 2012). Apps on mobile devices with permission to use the network may send third-party cookies to any destination with no restrictions at all. If users own an Android, there are many apps that have code from different advertising networks and analytics services. The Java code on the Android once it is compiled from third parties, is endowed with the same permissions as from the first party cookie. If the app has permission to access phone identifiers, a device ID is a unique, anonymized string of letters that identifies every individual smartphone or tablet in the world, then the third-party code can access phone identifiers also even though its use is often restricted by data privacy laws (Jung J et al, 2012). Accessing phone identifiers for a user capability is easily exploited by third parties to build a detailed profile of the user across many applications running on the same phone, as this creates detailed descriptions of users so companies can use this against them. The use of mobile activity is different from traditional browsing on computers in that the availability of censored data like images, audio, and location on mobile devices may be collected and sent to third parties if the application has any potential permissions to access it. Real world names and censored information can mean trackers can create a profile that is very personal for lots of individuals. Censored information or real-world names can be things like records of conversations or even where the user has been (Wetherall, D. et al, 2012).

2.3 THE HACKER

When a hacker finds a way to edit or manipulate a cookie, they can gain access to the user data that is stored within. The hacker can use this data to gain unauthorized access to users' accounts or even steal their identity. The amount of information a hacker is privy to is dependent on how users set their device permissions. When users set their devices to allow for maximal permissions, more of their information can be stored within their cookies, which means the hacker can access substantial amounts of personal information. Hackers that engage in session side sniffing, also known as cookie sniffing, can steal user's personal data, and many users do not know that setting cookies with maximal permissions increases a hacker's ability to sniff a cookie during browser and server communication. The continuous use of third-party cookies set with maximal permissions establishes a network that sends cookies back and forth between browser and the server. This process could potentially leak a user's PII, which is a major ethical issue (Fukuda, K. et al, 2021). Resultantly, user's must learn how to use their best judgment to manage their browsers and protect their safety. However, without more visibility or simplistic client tools that can provide this functionality, users are considerably vulnerable. Until there are more concrete laws and established best practices among developers, there is a need in the market for a tool that users can utilize to help them manage their cookies and secure their internet identities.

Disruptions such as sniffing an active session can lead to session hijackings and access to unauthorized sensitive data, economic loss, and damage to the reputation of the user or organization. If the site has a vulnerability to cross-site scripting (XSS) which is an attack where an attacker injects malicious executable scripts into the code of a trusted application or website, then the attacker can change the content of the website or even redirect the browser to another web page. with this a user is over 65 percent more likely to be hijacked (Fukuda, K. et al, 2021). As for the third-party context, the main issue is privacy.

Cookie's placement behavior refers to the cookies that the host places on the websites. When keeping the user's information to the least amount of sensitive information as possible, the amount of relative information with similar or near in size internet footprints differentiates on the browsing frequency that has been done. Preliminary work shows that data gathering, by expanding and using a larger number of websites and by reexamining cookie placements by both the first and third parties are determined by a more detailed model for using browsers behavior. These findings are also being adapted on information leakage to new methods for assessing and ensuring user privacy. The end users do not know or understand these possible hacking methods that can be used with their browser sessions.

2.4 THE TRACKER

The tracking ecosystem has grown exponentially in the last ten years. Building on standards and more advanced web tracking technologies, trackers usually try to attach a virtual identity to a unique user by collecting and monitoring a user's search behavior on the internet. Trackers obtain information from the third-party cookies, as the cookies are created by domains differently from a domain directly visited by the user. These cookies are accessible on any website that can use and load third-party domain resources. As trackers keep developing new ways to collect third-party data there have been proposals like the Privacy Sandbox project from Google Chrome to mitigate the usage of most third-party cookies to protect user privacy (Shadbolt, N., 2018). However, the prevalence of third-party cookies makes it a lot more complicated to overcome most of the countermeasures as third-party cookies are on almost every website a user visits. In an attempt to track users' activity more efficiently, a first party website can use a third-party tracking provider like www.tracker.net that is able to collect tracking information. When a user completes the signin on the first party website by inputting his or her

personal information, a tracking script then goes and reads their personal information. The script allows the tracker to match that user's browsing history across all websites, browsers, and devices without using third-party cookies. This mechanism focuses on personal information but also presents a constant web tracking technique based on this data transfer. The user data that is collected upon signin is used to check personal data leakage to any third-party domains (Shadbolt, N., 2018). In a study using www.tracker.net it was found that the results and the implications of this are not good for user privacy as over 40 percent of popular shopping websites that have first party services leak to third-party receivers, one of the most common is Facebook.

Also on www.tracker.net users have the capability that allows tracking providers to identify a tracking mechanism and persistently track user's through cross site and cross browsing, this is useful as it evaluates how a web application or website functions across different browsers, (Shadbolt, N., 2018). Using this technology, users can analyze the presence of personal information leakage tracking. User's may discover the prevalence of tracking providers that leverage their private information to actively track user activities. This tracking method makes the user especially vulnerable, because using tracking mechanisms that retrieve data and information stored on a user's computer can make the user feel like their information is being stolen and their privacy is being violated.

There are multiple methods commonly used by third-party trackers to analyze cookie synchronization that can bypass same origin policies on the web, and explore the unique identifier stored in a cookie or embedded as a parameter in a URL. This is a known method for leakage detection as it involves having the user's personal information leaked based on the poorly coded login forms that expose sensitive information in the URLs. More accurately, these forms submit user information to a first party web server using the GET method. For instance, if www.thesite.com has a sign-up form that uses the GET method to submit a user's email address, the user's browser then creates a request with the form parameters containing the email address. In the case that www.thesite.com includes a third-

party www.tracker.net in its authentication flow, a request is sent to this third-party because the reference header is sent with a request for a remote resource. For example, their data could be sent out making fake user profiles and their email addresses could be stolen (Shadbolt, N., 2018). According to the research conducted on the websites leaking personal information, the first 130 first party websites that were looked at and had leaked personal information to third parties obtained user consent in the authentication flow as a user requirement. Unsurprisingly, all of these websites provide users with a form to sign without clarifying how their information is being used. This relationship is a violation of trust and transparency, and it leaves users particularly vulnerable. As can be seen in the figure below the use of third-party and third -party trackers is extensive in many countries around the world.

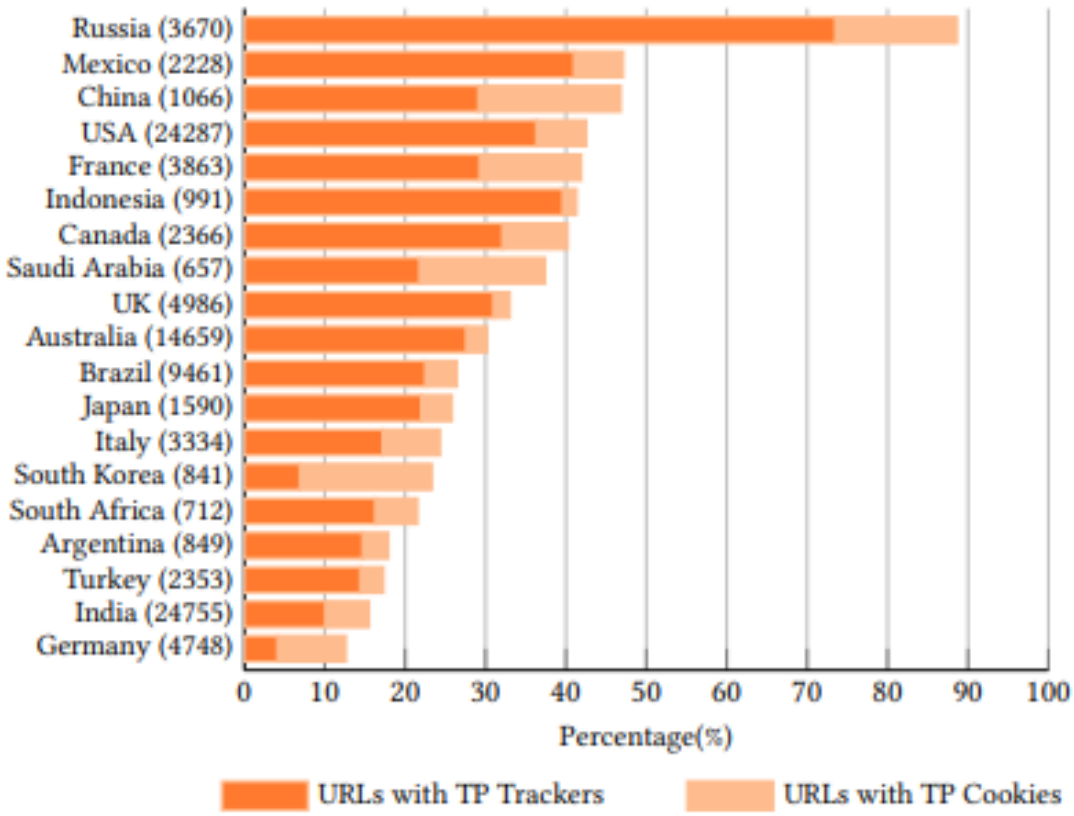


FIGURE 2: PERCENTAGE OF URLS THAT CONTAIN THIRD-PARTY (TP) AND THIRD-PARTY TRACKER (TPT) COOKIES. (SHADBOLT, N., 2018).

2.5 DOES TRACKING PROTECTION ACTUALLY WORK?

Reduce a user's exposure to tracking; if the browser has built in privacy extensions such as these two ways Ghostery which monitors different web browsers that are being called from a particular web page and matches them with a library of data collection tools or uBlock Origin which is an ad-blocker counter and trackers blocked. These features are effective, but only 237 sites of the websites that were researched which are less than 0.5% users actually have a

measurement to block all third-party cookies (Narayanan, A. et al, 2016). The most interesting discovery from the websites is that the majority of top third-party cookies sync with at least one other party (web browser). That cookie syncing is definitely under privacy concerns because it shares the data of users between platforms to ensure the same user is recognized across different devices and platforms, finding that third-party cookies are well connected by synched cookies. Specifically, of the top 50 third parties that are involved in cookie syncing, the probability that a random pair will have at least one cookie in common is 85%. The corresponding probability for the top 100 is 66%. (Narayanan, A., 2016). The same user might not want to be recognized or tracked across different websites causing the issue.

2.6 SERVER COOKIE

A server cookie occurs on the server side and not the user's side. A server may send randomized information, (the cookie) in a Set-cookie response header to users. When a user leaves and comes back to the browser, the arbitrary information could include anything from a user identifier to a database key, or whatever the server needs so it can continue where it left off on the server. A server cookie is used to tell if two requests come from the same browser, for example keeping a user logged in. Under normal circumstances, a group working together (cooperating client) returns the cookie information word for word in a cookie header, one of its request headers, each time it makes a new request to the same server. The server may choose to include a new cookie with its responses, which would supersede the old one. There is an implied contract between a server and user, the server relies on the users to save the server's state and to return it on the next visit. To correct a frequent misstatement in early press stories, cookies do not arise from some insidious invasion of a user's computer or hard drive by an external intruder. Rather, the user's browser stores only those cookies it receives from a server it has visited. A website

cookie, then, is the piece of information that the server and client pass back and forth. The amount of information that is passed back and forth is generally small, and its content is at the discretion of the server. In general, simply examining a cookie's value will not reveal what the cookie is for or what the value represents. Therefore, when it sends a cookie to a client, a server may specify, in a constrained way, the set of other servers to which a client may also send the cookie in subsequent requests.

Resulting from the global pandemic, governments around the world have shifted to providing online services and digitizing in ways that meet the needs of their citizens. There are plenty of benefits to this, such as low operating costs, and marketing is much easier. For the increases, the danger for users of being tracked through websites. Being tracked through websites has become a great concern as the government only provides information on the Covid 19 pandemic and not the public (Laoutaris, N. et al, 2022). Regardless, it has been found that 90% of government websites create cookies that are tracked by third parties. Non session cookies that are created by trackers can last a long time on a user's device, which can be pulling a user's information even if not on the browser (Laoutaris, N.et al, 2022). Users need to understand the cookies on these sites because they are used often and have relevant info. It seems that promoting good regulations like GDPR (government sites) are not clear of trafficking targeted regulations. The government and international organizational websites that share public health information related to the pandemic, are not held to the correct high standards that protect user's privacy. Further analysis shows that trackers are widely present in such websites. The external content from social media and third-party services shows how difficult it is to apply any type of data protection because the user's data is being passed around through different websites so some who have good regulations cannot stop other websites from passing the users information. (Gotze M et al, 2022). Innovative technology and systems need to be implemented so there can be more privacy for users especially in matters that concern their health and safety.

2.7 TRACKING THE TRACKERS

In order to prevent third-party trackers from learning personal information, users can install systems that provide anti-tracking as an added or supplementary feature to the devices. For example, users could install AsBlock Plus, which performs mainly to block advertisements in addition to other anti-tracking capabilities. Another system, Noscript, takes a more conservative approach by preventing any and all Javascript from being executed in a user's browser (Pujol, J.M et al., 2016). Noscript can block all forms of communication between the user's browser and a third-party tracker. However, this approach is deeply flawed as most sites rely heavily on Javascript for regular functions. This difficulty that occurs with Noscript highlights a fundamental tension and tradeoff, preserving privacy while maintaining usability (Pujol, J.M et al., 2016). Implementing anti-tracking features may also cause harm to website appearance and functionality, making it difficult to incorporate security measures with minimal breakages. Keeping breakages minimal is important for user satisfaction and retention as well as maintaining privacy protection. For example, if the site stops working or is broken, the user might try to solve it by creating rules in the anti-tracking engine to disable trackers (Pujol, J.M et al., 2016). These rule changes might open gaps in the security protection for user's, who may not understand what they are adding or how it can affect them. Creating rules for these organizations would lower the number of unsafe trackers following each user.

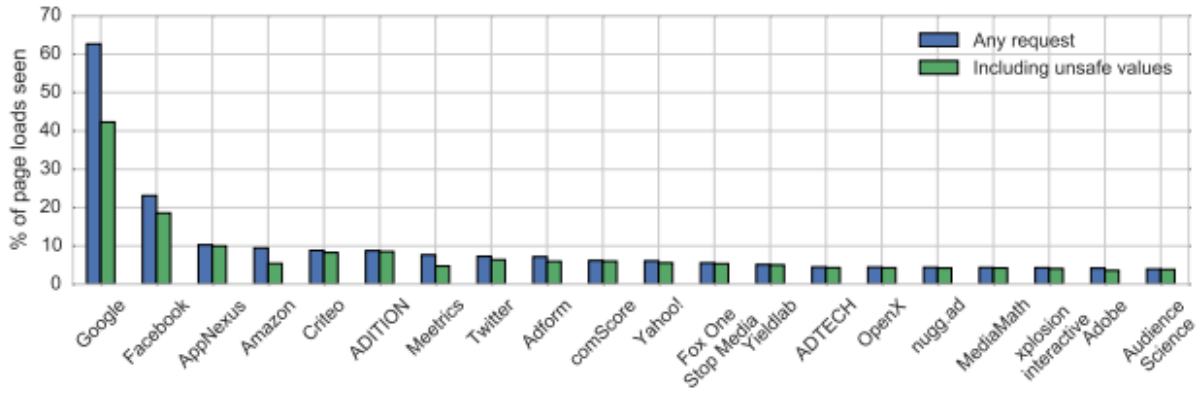


FIGURE 3: TOP 20 ORGANIZATIONS BY COMBINED TRACKER'S REACH. (PUJOL, J.M ET AL., 2016).

NOTE On Figure 3: The ownership of a tracker is based on Disconnect's blocklist. The first column accounts for the percentage of page loads in which a request to the potential tracker is issued by the user's browser. The second column is when the request also contains unsafe data.

2.8 PRIVACY LOSS

The Increased dependence on the Internet for a wide variety of daily transactions causes access trails to be left in many locations. (Wills, C.E et al., 2007). A browser-based approach is intriguing as disabling cookies can be applied at the source of requests and are custom to the individual preference of the user. Disabling cookies can be done by applying to all third-party servers, this is the most commonly provided "privacy" technique by browsers such as Firefox and Internet Explorer. (Wills, C.E et al., 2007). Another technique for disabling cookies is to disable JavaScript execution, this is not technically labeled for privacy in either Internet explorer or Firefox, this will eliminate execution of JavaScript code. This NoScript Firefox extension can be used together with the technique to allow JavaScript execution temporarily or permanently for specific domains, this technique is one of the best to disable cookies as Javascript execution is helping pass cookies on. Another one for disabling cookies is filtering ads; this is

provided by Firefox extension AdBlock Plus allows URLs that match regular expressions to be ready to be downloaded (Wills, C.E et al., 2007). This is not specifically designed for the protection of privacy, this extension can be used to block undesirable URLs, Common filter rulesets do block some servers known to do aggregation.

2.9 WEB PRIVACY ATTACKS

Without comprehensive laws or direction given to users, many do not know that their private information can be tracked across browsers. Whenever a web browser leaks its long-term browser state to outside parties, the user then has a greater risk of being tracked (Mitchell, J.C. et al, 2006). While each user may have their own standards regarding the types of tracking that might be acceptable to them like a pre-programmed email address insert, the standards are often based on the user's knowledge of a site as a distinct location. A site is defined as a fully qualified domain name and all the pages hosted on it. It is also possible to define a site more specifically, as a path on a particular domain, or more specifically, as a partially qualified domain name; the corresponding tracking techniques would differ only in implementation details. Users often do not know that their web activity might be tracked from many different vantage points, starting from a certain single session tracking site to many different tracking that is across sites that do not cooperate with each other. There are two types of tracking that users may experience, either single session tracking or multiple session tracking (Mitchell, J.C. et al, 2006). Single session tracking is an embedded query parameter in URLs to get common knowledge as user's click around a website. Single session tracking can, for example, sites can embed query parameters in URLs to identify users as they click around the site and track them as they follow links to

other cooperating sites. Multiple session tracking allows a single site to gather information on a visitor over a few visits. It is not possible for a browser to allow cooperative site tracking such as single site tracking and multiple site tracking cannot work together.

Another tracking mechanism is Cooperative tracking; this allows cooperating sites to build a history of a visitor's activities on all the websites, even if they visit the website separately or during different browsing sessions (Mitchell, J.C. et al, 2006). Resultantly, the user's personal information will be linked with different activities at a different site such as email addresses can be used for a login or to recover login information for a user, even if they are not related at all. Third-party blocking does not defeat this kind of tracking. Semi-cooperative single-site tracking is allowing an attacker's site to determine info about a visitor's activities at any other site that is being targeted. For example, a forum may allow users to post remotely hosted images in areas but does not want the images to be "anonymous" as users go from one page to another. Semi-cooperative single-site tracking is consistent with the same origin principle but may be undesirable for a visitor or a targeted site. It is also possible to allow some types of cross site content without allowing semi-cooperative single-site tracking. There is also semi-cooperative multiple site tracking which is remarkably similar to semi-cooperative single site other than that the track can be across multiple targeted sites, even on the attacker's own website (Mitchell, J.C. et al, 2006). Lastly, non-cooperative tracking is what allows one website to determine a user's activities at another targeted site without any information from the target site. The diverse types of tracking mechanisms mean there are different ways of being tracked, it is useful knowledge as a user to understand how each one works. More regulations on these trackers will lead to safer and easier.

2.10 IDENTIFIERS

Users are identified with the help of identifiers, a wide variety of data points can serve as identifiers, ranging from the users IP address to a device's characteristics. Fingerprinting is a huge concern amongst privacy specialists as it is used maliciously to track users in a covert manner bypassing user choice and overcoming ways of certain methods of tracing (Kristol, D.M., 2001.). Users cannot decline to be fingerprinted. Every user is always being traced in some sort of way. There are so many ways of data points that can be used to fingerprint a device, most cannot be modified by the user. At the same time, the browsers efforts to minimize fingerprinting are making this process more difficult and less effective but truly it cannot be fully blocked. This is because this is fundamental to how the internet works. Device fingerprints are stored server side so consequently users cannot delete or reset anything to prevent fingerprinting even browsing incognito or private modes make zero difference. In fact, the more privacy aware someone is, the easier it can be to track them through fingerprinting (Kristol, D.M., 2001.).

2.11 THE WEB NEVER FORGETS

Tracking being difficult to control and the need for legislation that helps to explain these issues to users. Canvas fingerprinting is a web tracking technique that uses a combination of system attributes to create a unique identifier for the user. Canvas fingerprinting also uses the browsers canvas API to draw invisible images such as an exposure to light similar to that of a photosensitive material such as photographic film. Also extracting a persistent long-term fingerprint without the user's knowledge. Canvas API can be used for animation, game graphics, data visualization, photo manipulation, and real time video processing. There does not appear to be a way to automatically block canvas fingerprinting without false positives that block legitimate functionality such as if all internet users randomized their canvas fingerprints, this way it is hard to pinpoint a single user. (Diaz, C. et al, 2014). Even a partial fix for canvas fingerprinting requires a browser source code patch to reduce the security risk for users. The Evercookies actively circumvent users' deliberate attempts to start with a brand-new profile.

Evercookies are a persistent web browser cookie technology deployed by websites to retain and reproduce cookies that have been manually deleted or altered by a user. Cookie syncing is a workaround to the same origin policy, allowing different trackers to share the user's identifier with each other. Other than being hard to detect, cookie synchronizing enables back-end server to server data that merges hidden from the public view (Diaz, C. et al, 2014). Public view, which means that governmental laws are needed more than ever to protect vulnerable users.

3.0 CURRENT COOKIE LAWS AND REGULATION INCLUDING THEIR FAILURES

3.1 WHAT IS BEING DONE TO STOP COOKIE INFORMATION BEING SHARED

In response to the development and proliferation of trackers embedded in cookies and the lack of wide-scale deployment of a user's defense against tracker controls, various efforts have been made by mobile OS platform developers to address the risks of privacy. Mobile application developers must follow a series of rules pertaining to third-party trackers in order for their apps to be listed in the App Store or Google Play Store. Specifically, Google and Apple can exert control over the apps that appear in their respective stores, and both companies have agreements that limit third-party tracking (Muthukrishnan, S. et al, 2016). For users, these application rules mean that they are able to shift from app to app without encountering large amounts of trackers, and this experience using apps contrasts their traditional internet browsing experience and the many ways they encounter trackers as they shift from one browser to the next. Because mobile OS platform developers have the ability to impose industry self-regulation controls like kicking an application off the platform entirely, users can have different experiences with cookies depending on their device. Therefore, industry led self-regulation

controls attempt to strike a balance between protecting users from malicious behaviors and creating a permissible environment that optimizes user experiences. These self-regulation efforts have a significant level of enforcement worldwide, especially in Europe which is one of the best data legal regimes. With the European Union's General Data Protection new enforcement powers, including the issuing of larger fines and the scope for suspending processing, may end the activities of third-party cookies (Muthukrishnan, S et al, 2016). For example, the specific identification and purposes of third-party trackers will have to be made clear to the application user. This is a step in the right direction as punishments are now being set in place for third-party tracking, disincentivizing sharing and storing private user data.

3.2 EUROPEAN UNION'S SAY

The European Union's General Protection Regulation (GDPR) came into effect in 2018, this is a privacy regulations service that can be used to protect any service or company collecting or processing personal data in Europe. Resulting from this law, many companies across the EU had to change their data handling process ways, privacies, and consent forms to comply with the new GDPR requirements (Holz, T. et al, 2018). This change was monitored by analyzing 28 member states of the European Union. All the countries in the EU monitored the 500 most popular websites from December 2017 to October 2018. Countries found that 15.7 percent of websites added new policies by May 2018 for the GDPR, and this ultimately resulted in more than 84.5 percent of websites updating their privacy policies. Just over 70 percent of the websites with the existing policies updated them close to date. After May 2018, this improvement slowed down massively, but it resulted in over 60 percent of websites in Europe creating a cookie notice bar, 16 percent more than in January 2018 (Holz, T. et al, 2018). This analysis of the response to GDPR rules by European websites shows that these websites abide by the implementation of the GDPR rules and are keen on following them and cooperating to manage third-party cookies by implementing

web security mechanisms. While many companies already had internal regulations, a large majority of them made impactful changes like incorporating the cookie consent banner, which is a visible measure to protect and inform users. The cookie consent banner is now available on 50 percent of all European websites, which is a step in the right direction towards securing internet privacy for users. However, this increase in so-called protection may lead to a false sense of security and privacy for some users, as few websites offer their user's descriptive information that informs them how their data is being collected, stored, and tracked. Additionally, because the GDPR rules are so new, many regulators have failed to provide clear guidelines to websites (the GDPR shown in table 3 is only on a slight rise). These guidelines should define what cookies are, the implications for users, and what sorts of activities require consent (Holz, T. et al, 2018). Because of this lack of direction from regulators, websites may not implement all of the requirements stipulated by the GDPR and this will inevitably impact user safety and security.

	Top list					TLD			
	n	pre	post	diff		N	pre	post	diff
AT	455	33.0 %	55.2 %	22.2 %	.at	132	45.5 %	69.7 %	24.2 %
BE	460	40.9 %	61.1 %	20.2 %	.be	141	59.6 %	78.7 %	19.1 %
BG	451	37.9 %	60.5 %	22.6 %	.bg	166	52.4 %	71.7 %	19.3 %
CY	432	26.4 %	50.2 %	23.8 %	.cy	58	13.8 %	27.6 %	13.8 %
CZ	459	34.0 %	52.7 %	18.7 %	.cz	251	44.6 %	58.2 %	13.5 %
DK	447	41.2 %	68.9 %	27.7 %	.dk	174	72.4 %	87.4 %	14.9 %
DE	455	26.2 %	49.0 %	22.9 %	.de	172	42.4 %	64.5 %	22.1 %
EE	441	9.5 %	35.8 %	26.3 %	.ee	132	14.4 %	35.6 %	21.2 %
ES	429	41.5 %	64.3 %	22.8 %	.es	86	72.1 %	84.9 %	12.8 %
FI	462	27.5 %	53.9 %	26.4 %	.fi	145	37.9 %	55.9 %	17.9 %
FR	453	49.2 %	66.9 %	17.7 %	.fr	139	77.0 %	87.1 %	10.1 %
GB	463	37.4 %	67.0 %	29.6 %	.uk	108	58.3 %	82.4 %	24.1 %
GR	443	40.0 %	59.8 %	19.9 %	.gr	233	56.7 %	69.1 %	12.4 %
IE	447	21.3 %	64.2 %	43.0 %	.ie	104	17.3 %	87.5 %	70.2 %
IT	423	21.3 %	66.7 %	45.4 %	.it	174	30.5 %	90.8 %	60.3 %
HU	440	46.4 %	62.7 %	16.4 %	.hu	228	67.1 %	76.3 %	9.2 %
HR	430	28.6 %	54.7 %	26.0 %	.hr	141	48.9 %	70.9 %	22.0 %
LV	434	16.8 %	41.9 %	25.1 %	.lv	126	38.1 %	61.1 %	23.0 %
LT	452	27.0 %	47.3 %	20.4 %	.lt	174	50.0 %	63.2 %	13.2 %
LU	440	24.8 %	51.8 %	27.0 %	.lu	61	36.1 %	57.4 %	21.3 %
MT	446	25.8 %	58.1 %	32.3 %	.mt	46	21.7 %	43.5 %	21.7 %
NL	459	37.3 %	54.2 %	17.0 %	.nl	115	85.2 %	87.8 %	2.6 %
PL	462	53.9 %	68.6 %	14.7 %	.pl	256	75.4 %	83.2 %	7.8 %
PT	430	31.4 %	53.7 %	22.3 %	.pt	116	52.6 %	65.5 %	12.9 %
RO	434	30.2 %	53.5 %	23.3 %	.ro	160	52.5 %	73.1 %	20.6 %
SE	459	33.3 %	63.6 %	30.3 %	.se	166	50.6 %	78.3 %	27.7 %
SK	438	42.2 %	56.8 %	14.6 %	.sk	189	60.3 %	69.3 %	9.0 %
SI	451	43.9 %	64.1 %	20.2 %	.si	132	75.8 %	77.3 %	1.5 %
Total	6357	46.1 %	62.1 %	16.0 %		4125	50.3 %	69.9 %	19.6 %
					.com	1915	28.7 %	50.7 %	22.0 %
					.net	248	25.4 %	35.5 %	10.1 %
					.ru	148	5.4 %	6.7 %	1.3 %
					.org	119	13.5 %	23.5 %	10.8 %
					.eu	43	23.3 %	37.2 %	13.9 %
					.tr	32	6.3 %	6.3 %	0.0 %

TABLE 3: Availability of cookie consent notices in the top 500 websites by country, pre- (January 2018) and post-GDPR (after May 25, 2018) (Holz, T. et al, 2018).

3.3 WHAT HAS TO BE DONE WITH PRIVACY?

To address the rampant misuse of cookies, the interconnected relationship between individuals, the private sector, and the government must be acknowledged as a serious issue. Particularly because user experiences are directly controlled by big corporations and businesses who leverage user data in often exploitative ways to earn revenue, the involvement of the government in the maintenance of these relationships is very controversial. In fact, many companies have made trading private user data their main source of revenue, which lends to a manipulative and tactical relationship between the user and the company. The framing of user data and privacy is political and controversial, an extension of state power, impacts measurable efforts to protect user privacy and is what allows companies to profit off using user data (Etzioni, A., 2011). Specifically, the term “more government regulations” and the idea of expanding governance in an esoteric capacity informs a certain politicization of user protection and the debate between what is and what is not considered to be an internet normality (Etzioni, A., 2011). It is essential that users overcome this blinding politicization and recognize the implications of unbounded profiling. Users should be wary of claims for self-regulation because this assumes that corporations can be trusted to self-regulate and act ethically in a marketplace that can potentially cause harm and violate their safety and security. Extraordinarily little attention has been considered towards information being fungible, that would be considered Privacy Violation Triangulation (PVT) which may serve, if combined with laws that add “patches” to the current patchwork of legislation that can be used to cover new technical developments like social media. If it is possible there would be less reason to prevent the government

from grabbing data from corporations. This means corporations would be limited to less sensitive information, then the PVT of the innocent public would be banned (Etzioni, A., 2011).

3.4 COOKIES SECURITY FAILURES

This article entitled “Pre-Hijacked accounts: An empirical study of security failures in user account creation of the web” provides useful information on account hijacking and what it means for user’s and their privacy. It primarily studies the ubiquity of user accounts in websites and online services that makes account hijacking a serious security concern. Previous research has not encompassed the process of account creation while focusing on the various techniques attacker’s use to gain access to a victim’s account. A new trend highlighted in the research is attacker’s using techniques like Cross-Site Request Forgery (CSRF) to trick victims into changing their account passwords. The trend towards federated authentication which allows authorized users to access multiple applications and domains using a single set of credentials, in which the user directly sets a password, and the federated via an Identity Provider (IdP) (e.g. Single Sign On SSO), adds additional complexity and broad challenges for user’s as many services now support both this federated approach and the classic approach .

Federated attacks make users particularly vulnerable because they are simplistic and look like a password-reset request coming from the original browser. The distinctive feature of pre-hijacking account types of attacks is that the attacker performs some action before the victim creates an account (Hormozi, A.M., 2005). Once a new account is created by the victim, the attacker has the simple task to gain access after the victim has created or recovered the account. Researchers have also identified five diverse types of account pre-hijacking attacks. The five distinct types of attack are Classic-Federated Merge Attack, Unexpired Session Attack, Trojan Identifier Attack, Unexpired Email Change Attack and the Non-verifying IdP Attack (Paverd, A. et al, 2022). All these attacks rely on different site

characteristics and vulnerabilities, but they do have some similarities regarding the phases they take place in.

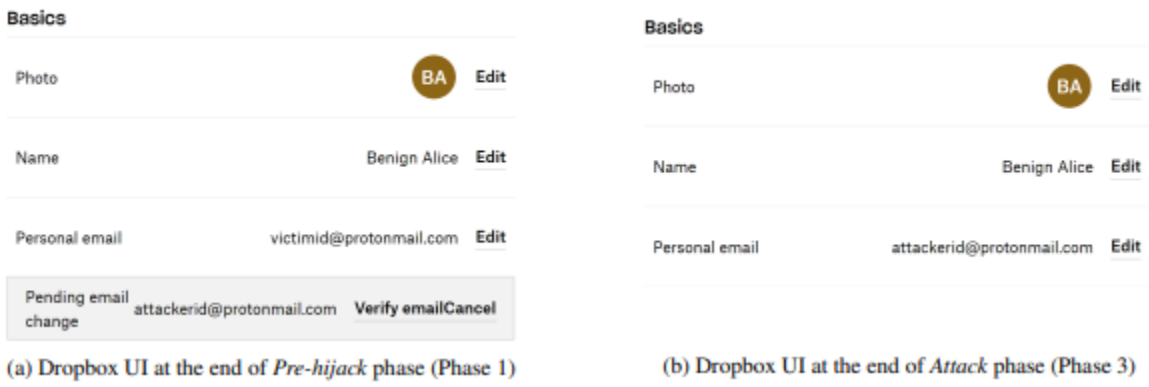
All account pre-hijacking attacks consist of three phases: 1) Pre-hijack, 2) Victim action, and 3) Attack (Hormozi, A.M., 2005). The main requirement during the pre-hijack phase is that the victim must not have created an account with the target service using that identifier. In the victim action phase, they either create or recover their account at the target service using the same identifier used by the attacker in the pre-hacking phase. Although many sites send email notifications in some of these scenarios, many users do not recognize the hijack for what it is and even in that process the hacker has a trick to circumnavigate being discovered. In the attack phase, malicious actions can be taken on behalf of the victim user's account (Paverd, A. et al, 2022).

To find out how widespread hijacking vulnerabilities are, Paverd, A, analyzed 75 popular global services that supported user accounts and found that at least 35 of these were vulnerable to one or more account pre-hijacking attacks. Whilst some of these attacks may be noticed by attentive users, others were completely undetectable from the victim's perspective. The experiment was conducted by manually creating accounts as an attacker then re-creating the account as a user. The results were disclosed to each site so that they could fix their vulnerabilities via their respective disclosure channel and enhance user security.

As a known vulnerability that cookies can be injected by HTTP response into subsequent HTTPS requests, and from one domain to another related domain (Weaver, N. et al, 2015). In 2013 GitHub migrated their services from github.com to github.io after they saw a threat of cookies be injected from or to a shared domains that are with users they don't trust.

Paverd, A., also investigated the root cause of these vulnerabilities and presented a set of security requirements to prevent such vulnerabilities from arising in future. They identified the root cause

as the failure to verify ownership of the claimed identifier meaning that the user has been on the website previously. Although many sites do perform this type of verification, they often do so asynchronously, allowing the user to access certain features of the account before the identifier has been verified. It was found that the majority of attacks could be prevented if the site or IdP sent a verification email to the user-provided email address and required successful verification before any further actions associated with the account**.** This email verification should also be completed for password resets, account mergers, email changes and deleting in-active accounts (these issues are shown in figure 4 below). Additional security measures are Multi-Factor Authentication which is a multi-step login process which requires more information than a password (MFA). Most notable is the fact that many of these vulnerabilities are avoidable when site developers take additional steps to check and secure their sites. Site developers have the ability to create test scripts to check for the main pre-hijacking vulnerabilities, using a similar automated approach that was used in to create the initial accounts. In this way, site developers are attacking their sites to check for potential flaws and security issues.



(a) Dropbox UI at the end of *Pre-hijack* phase (Phase 1)

(b) Dropbox UI at the end of *Attack* phase (Phase 3)

FIGURE 4: DROPBOX UI OF THE VICTIM'S ACCOUNT DURING THE UNEXPIRED EMAIL CHANGE ATTACK (PAVERD, A. ET AL, 2022).

3.5 PRIVACY ANALYSIS

Online tracking is evolving from browser and device tracking to tracking peoples. A whole new level of trafficking has arisen by way of users accessing the internet through multiple devices. New forms of advertising are aimed at crossing this boundary between a device and the browsers the user searches on (Jebara, T. et al, 2017). Online tracking seeks to combine the input from various data sources, which then can make a user profile to follow the user around to different websites. Using data from a cross-tracking device, can help reveal what an individual likes to search, which is far more invasive and particular than HTTP cookies or other classic and more tracking mechanisms (Jebara, T. et al, 2017). In a study conducted by researchers Jebara, T. et al, the researchers examine cross-device tracking mechanisms and techniques as well as the privacy implications for users. Using a cross-tracking dataset collected from 126 different internet users, the researchers studied cross device tracking on desktop and handheld devices. The increase in technology power that companies are using to take data from more than a single device is way more than they used to be capable of. In the end, cross device tracking is an emerging tracking paradigm that challenges current privacy implications, using the cross device set that was made in the study, the correct tracking algorithm and the evaluated relevant features and parameter settings grounded in a review of public information of the practices of cross device companies. For some users, it appears that the companies can learn more from each individual device data. Cross device tracking on the internet is extremely high already (Jebara, T. et al, 2017). This means it is more important for companies to be transparent about their practices. Some things are certain, IP addresses are a massive way for correlating devices. Ultimately cross device tracking is part of something way bigger, the Internet of Things, the increase of inter connectivity between devices. Increasing cars, buildings, and appliances, these are all things that need to be connected to the internet, these are all interacting with other devices nearby. However, the deployment of privacy within the Internet must be ensured by transparency and practicable control mechanisms (Jebara, T. et al, 2017). A solution to this issue of transparency could be an intelligent personal privacy assistant that is connected to all the services and devices of one user.

3.6 CHALLENGES IN SUPPORTING PRIVACY

Social navigation systems are a form of social computing. They are a promising approach for supporting privacy and security management. Social navigation systems can provide users with easily understandable guidance when making security and privacy decisions. These systems provide information that is user-friendly and not overly technical or complicated (Mynatt, E.D et al., 2009). There are currently two prototype systems that are working to coordinate social navigation and user knowledge, teaching user's how to manage their security and privacy on the internet. The Acumen system employs social navigation to address, managing internet cookies, which is a common privacy activity that fundamentally confuses user's (Mynatt, E.D et al., 2009). The Bonfire system uses social navigation to help users manage their personal firewall which will lower the chance of cyberattacks against the user. Acumen and Bonfire both represent a potential for users to learn and practice privacy management. Regardless, there are still many challenges that inhibit the success of the systems (Mynatt, E.D et al., 2009). Due to features of these domains, individuals may misuse community data when making decisions. For example, an employee can copy data to a flash drive for personal use but lose it, resulting in a data leak. Leading to incorrect personal mistakes. Data, and "herding" behavior is an example of an economist's term of an informational cascade. Researchers have conducted research by understanding this phenomenon in these terms, developing, and presenting two general approaches for mitigating herding which is where users follow others and imitate groups rather than deciding independently, in social navigation systems that support end-user security and privacy management, mitigation by algorithms and mitigation by user interaction. Mitigation via user interaction is a promising approach in social navigation

systems (Mynatt, E.D et al., 2009). The concept of mitigating cascades in social navigation systems for privacy and security management has an impact on users. Continuing to practice and further the study of the cascade's concepts can help clarify its scope and most importantly its utility. Acumen and Bonfire had experiments done on them to evaluate how often and under what conditions cascade from each system (Mynatt, E.D et al., 2009).

3.7 THIRD-PARTY TRACKING

Third-party tracking refers to the practice by an entity other than the website directly visited by the user, traces or assists in tracking the visit to the site. Page Fetching which is fetching web pages using headless chrome and storing all fetched resources including Java files occurs, an HTTP request made by the client, to a named host, and located on the server is made for the site for a URL in a new top-level execution context for that site. The top-level execution context handles the entire transformation and execution of the code (Wetherall, D. et al, 2012.). The HTTP response contains resources of several distinct kinds such as a document, photo, or anything else. These are processed for display, and which may trigger HTTP requests for additional resources. The process will then continue over and over until it is loaded with text, images, sound, video, or other multimedia files. Execution of a website can embed information or content from another domain in two ways. One of the ways is the inclusion of an Iframe which is a HTML element that loads another HTML page within the document, this delegate a portion of the screen to the domain from which an Iframe is kept, this is known as the third-party domain (Wetherall, D. et al, 2012.). The other way is the Origin policy is a security mechanism that restricts how a document, or a script loaded by one origin can interact with a resource from another origin, which ensures

the two domains are isolated. Scripts that are running on the iframe run in the context of the third-party domain. When a page includes a script from another domain the script will run then on the first party domain, however, this does not occur on the script source (Wetherall, D. et al, 2012.). These scripts interact with the system generated graphics windows buttons and menus to simulate user actions. Every computer user uses scripts of some kind, even if they are not aware of it.

3.8 TECH PLATFORMS AS PRIVACY REGULATORS

User privacy has greatly given lawmakers around the world to follow EUs example of GDPR, the USA has provided the CCPA which grants California consumers greater access over their data and secure new privacy rights for them. Users have the right to know about, under the CCPA law, the information a website or business collects about them and how it is used and shared (Karanikioti, T. et al, 2020). Users also have the right to opt out of transferring their PII to other companies and websites so that users can stay more protected. Recently the CRPA further strengthened the data privacy framework which entered into full force on January 1st 2023, by making it more difficult for lawmakers to get rid of privacy laws in future so new and improved privacy laws on the internet can come and stay so less personal information will be taken, including the right to correct inaccurate personal information, and the right to opt out of automated decision making and the right to restrict the use of sensitive personal information. Users wanting more control over personal information led to the creation of the California Privacy Protection Agency, an agency exclusively focusing on consumer privacy which can protect more users for safer internet use (Geradin, D et al., 2020). Remarkably the GDPR caused a change

in the global standard for data protection and privacy by making a change in the law and giving users more power. Another substantial change to their privacy information was Google and Apple, as Google is the leading provider of ad services across every part between marketers and publishers. Apple is the second most popular browser, which has lots of ad services which can cause issues between the publishers and ad marketers (Karanikioti, T. et al, 2020). Company regulators should lay out the information they collect from users and the reasons for doing so to make the users feel more protected. The issue between ad marketers and publishers is the place to display that message with a viewership that the advertiser is interested in converting.

4.0 POTENTIAL IMPROVEMENTS IN THE USE COOKIES

4.1 THE BLOCKERS

Network based blocking methods such as DNS blocking which uses address-based blacklists in order to block access to certain domains, which were in use long before browsers supported the notion of plugins and extensions (Weippl, E. et al, 2017). In the context of blocking trackers including ads, DNS blacklists are distributed in a form of a hosts file. The host files which are used to resolve a name into an address, translate a host name into its internet address. Host files are intended as replacements or extensions to the stock of operating systems, this is an OEM (Original Equipment Manager) operating system that a Samsung or Apple puts on a mobile device. DNS blacklists are mainly focused on blocking advertisements and trackers include the longstanding MVPS hosts, and Peter Lowe's list are ad and tracking

server blocklists. DNS blacklists have been around since the 1990s and are now finally conducting blocking in-app ads on mobile devices (Weippl, E. et al, 2017). This is beneficial for users as more of the web browsing nowadays is on a user's phone, meaning there will be less ads for users to deal with on the phone. The tracker method works independently of the used application but is a very well-known form of blocking that can be used to block entire domains or subdomains. For users this is beneficial as users are automatically rejecting messages from a block senders list.

4.2 HIDDEN WEB

To detect tracking on the sites that have been selected by researchers, they used webXray which users can download the software and it is compiled in Python code (Libert, T., 2015.). To detect the tracking, the first step is to list website addresses and then give them to the program. This list is then processed to ensure the addresses are all correctly formatted and not links to binary files and duplicates such as a .pdf or .xls as a user does not want extra files. Next, each site is relayed via the Python subprocess module to a command line instantiation of the “headless” web browser PhantomJS, in this context “headless” this refers to the fact the browser runs on a command line and does not require any graphical user interface which makes it quick as no graphics need to be loaded in order to test or retrieve information. This makes PhantomJS the most ideal for deployment of cloud based virtual machines (Libert, T., 2015.). PhantomJS provides a JavaScript API enabling automated navigation, screenshots user behavior, and assertions domain consisting of ordered a web address. A Java program which is responsible for loading the website, processing the page title and metadata, collecting cookies,

and detecting received HTTPS events and also HTTPS requests. PhantomJS is given 30 seconds to complete loading the page then the results are passed back to the Python script as JSON data and processing would resume. The data about the page such as the title and metadata are stored in the database and then HTTP requests are examined. PhantomJs permits the inspection of network traffic, making it suitable to have different analyses on the network behavior and performance. PhantomJs as its a “headless browser” has a smoother performance time compared to its main competitor Selenium.

4.3 OPENWPM COULD BE THE ANSWER

OpenWPM is a web privacy measurement framework researchers used to crawl the top million websites and track their abilities. Throughout the process of using OpenWPM to track each website's tracking abilities, researchers used image rendering to determine that many websites use fingerprinting methods such as third-party cookies to users this means they are being tracked on every website they go to, these fingerprinting methods are found based on image rendering (Pohlmann, N. et al, 2020). researchers also found that most companies use cookie synchronizing which allows them to analyze diff banner notifications and the effects of GDPR on privacy policies, most companies use cookie synchronizing which is when two ad platforms share and match the information they've gathered about the same user in separate databases. Researchers found over half the websites that were found to have a consent button notice, only very few offer the users much of choice because users have to accept to use some pages (Pohlmann, N. et al, 2020). Measures of the GDPR like the cookie consent dialog have been studied to a high degree to see how to store cookies on a user's browser, websites must ask for their consent. This was studied to determine the usability, for the impact on cookie settings. It is found

that websites do not set cookies when a user from the EU visits the website but a cookie is set but when the user is in a country from outside the EU meaning when the cookie is set so the user can send information back to the server later (coming back to a web page with info saved but not complete). Using OpenWPM researchers have measured prominent websites and evaluated if the GDPR affects users' third-party usage (Pohlmann, N. et al, 2020). The authors have found out that overall, the usage of cookies declined but not necessarily the main part for that change.

4.4 THE CRACKED COOKIE JAR

In recent years, browsers have had support for security mechanisms that are designed to protect users from different cyberattacks. The most recent study done on browsers is called the HSTS, this can prevent HTTP cookie hijacking attacks (Keromytis, A.D. et al, 2016,). Additionally, Certificate pinning occurs when the browsers Chrome and Firefox use HSTS preloading mechanisms. Certificate pinning is an obsolete Internet security mechanism that allows HTTPS to resist impersonation by attackers using miss issued or otherwise fraudulent digital certificates. HTTP strict transport mechanisms allow for websites to make sure browsers only communicate through HTTPS meaning it is more secure. This is done through the Strict Transport Security HTTP header which is a widely supported standard to protect visitors by ensuring a user's browser always connects to HTTPS (Keromytis, A.D. et al, 2016,). HSTS is currently supported by all major browsers and a few mobile browsers to remove the common insecure practice of redirecting users from HTTP to HTTPS URLs. An important failure to note is during the user's first request before the HSTS header is available, which exposes the user to hijacking if sent over by an HTTP address. As a safety measure, the major browsers will rely on a list that is already loaded on the browser with information (Keromytis, A.D. et al, 2016,). The list will proactively instruct them to connect to domains over HTTPS. User's will then be secured during the initial request to a website. Websites can apply to be

on the list through an online request form. HSTS preloading is only supported by Safari, Chrome, Internet explorer, and Firefox. So, depending on the cyber attackers' abilities and resources, a user can be hijacked through different browsers.

4.5 USER AGENT

The Seamonkeys interest lies in the integration of various tools and is suitable for users involved in the web, who want to use the resources of the network. Company website owners gather information on the different users on their website (Desai, B.C., 2015,). By default, SeaMonkey allows both first and third-party to block all cookies for the originating website only. SeaMonkey is an email client that supports multiple accounts, junk mail detection, HTML message support and address books. Allowing third-party cookies from previous websites only, for the retention of cookies, it accepts cookies normally by default, the other options are except for current session only, accept cookies for (user specific) days, and ask for each cookie (Desai, B.C., 2015,). It is troubling to see that the majority of these browsers which have a significant percent of the browser market share among them have default settings which allow third-party cookies. SeaMonkey is a tool that is used to regulate third-party cookies, implementing more of these tools are needed as the companies are allowing third-party cookies.

4.6 PRIVACY AUDIT

Privacy audit: are procedures to ensure that the organization's goals and promises of privacy and confidentiality are supported by its practices. As a result, they protect confidential information from abuse and the company from liability and a public relations problem. Companies should go to greater lengths in studying the methods they use to collect consumer information (Baker, M., 2008). This in some cases, such as audit will probably lead to the conclusion that users should be informed that their information is being sold to third parties. Modern technology that enhances privacy rather than weakens it should be adopted if possible. The most important marketers and advertisements on the web could set a higher standard than what exists now (Baker, M., 2008). These new technologies include software that ensures being anonymous on the web.

The policy arena for online privacy is a global one, as an international regulation rather than just a U.S based public policy, which could likely be the long-term answer. The policy arena for online privacy is a long-term answer because the plan would have been agreed by multiple sets of groups. So future goals should be for input across nations. This fundamental agreement between Americans who think the government is not trustworthy and Europeans who do not have much belief in self-regulation. The policy arena is showing that the much-needed compromise between the two continues to be assessed. Visions for the future of data collection and sharing do not align with the current situation In the EU and Us. There is not a fair marketplace or level playing field for users. Which means companies and politicians have more power on who makes laws for users. These are some of the few being offered Individual privacy consent, Innovative Self-regulation, and limited new regulation, these policies must be specific, informed, and unambiguous indication of the data subject wishes by the user indicates by a statement or affirmative action, signifying agreement to process

personal data relating to the user. Individual privacy consent is one major stipulation in the EU is the opportunity for users to ensure their initial consent for use of personal information. Details on how to move past this case-by-case method are very generic consent without giving much privacy is a huge question waiting to be solved (Baker, M., 2008). Innovative self-regulation has the FTC seeking the input of all major privacy groups in developing a workable privacy policy for the internet. The opt in requires a user to perform an affirmative action before they can be sent marketing emails, and opt out issue is having the users signed up to receive marketing emails by default and require an action from the user to opt out of receiving such emails continue to be a policy concern that websites would need to get the users agreement, instead of assuming that not saying anything is equal to consent. If users have the opportunity to hear or see information, they will make different choices regarding third-party cookies.

4.7 THE CLOUD

Cloud computing is the most popular form of IT today as it is the delivery of different services through the internet, including data storage, servers, databases, networking, and software. According to research from UC Berkeley on foundries that have been in the hardware industry, cloud computing is likely to have a similar impact. Further, researchers note that developers should design the next generation of systems deployed to the cloud as its cost saving, increased collaboration, more secure, and better disaster recovery (Molina, J., 2009,). Fears of the cloud by users like vastness and tracking capabilities have led users' perceived loss of control of sensitive data. From the perceived control measures that do not adequately address cloud computing’s third-party data storage and processing needs. These control measures are authentication, identity, access control, encryption, secure deletion, and data masking. The extended control measures from the enterprise into the cloud through the use of trusted computing which are technologies and proposals that aim to make computing more secure

through hardware and software enhancements. Also applied cryptographic techniques are symmetric key encryption, asymmetric key encryption, and public-key encryption. These measures should alleviate much of today's fear of cloud computing by creating a privacy policy reinforcement (Molina, J., 2009,). As regulations are set, it is imperative that users follow those rules so there is no misunderstanding when users accept or reject cookies.

4.8 BLOCKING

Researchers found that the online advertising trade groups have declined to provide a full understanding that 1% of all users decline cookies, user tools are important especially if online providers are not going to inform users about cookies in adequate ways (Mitchell, J.C. et al, 2012). As there are many different tools users can use as a blocking tool, some just completely block them but it is only a good solution if the user is more advanced (Mitchell, J.C. et al, 2012). The most effective tool to block cookies is the self-help tool's ability to block third-party content. Almost every web browser has a block list whether users have to get a subscription or get a configurable browser extension which is very easy to get for users. To understand the effectiveness of blocking, Mitchell, J.C et al tested by doing a baseline crawl to check the PS+1s to determine the third-party trackers on web browsers (Mitchell, J.C et al., 2012). The three values relative to baseline and averaged across all trackers: pages with an HTTP request to a tracker, pages with an HTTP Set-cookie response from a tracker, and cookies added less cookies deleted by a tracker. Refer to figure 5 for results.

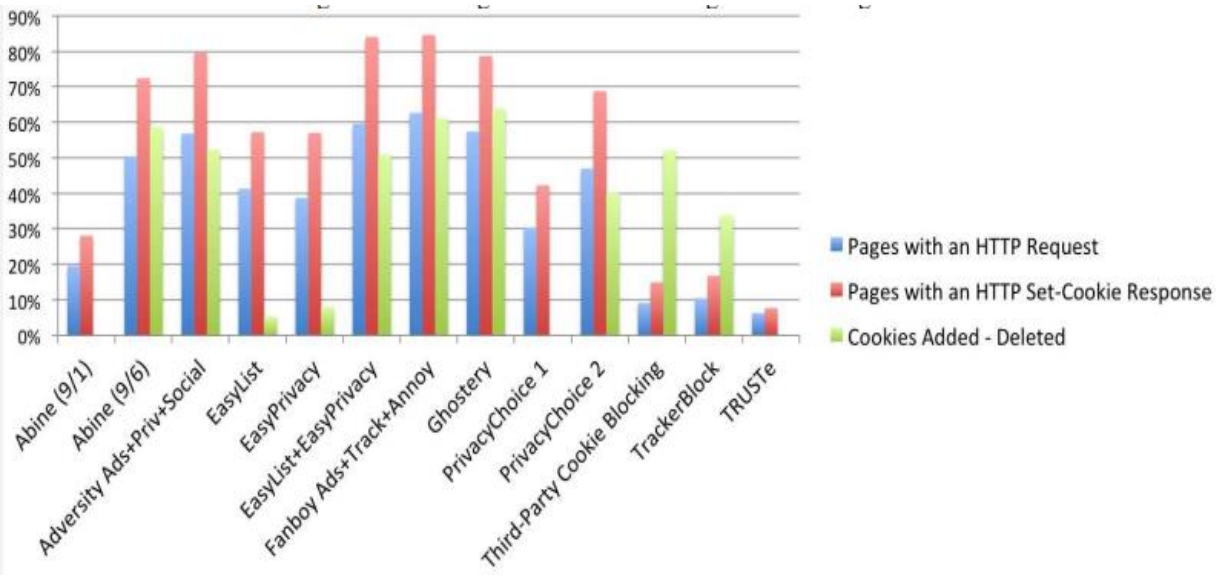


FIGURE 5: AVERAGE DECREASE IN TRACKING WITH BLOCKING TOOLS. (MITCHELL, J.C ET AL., 2012).

ANALYSIS

Once the current cookie landscape is somewhat understood, from a personal security mindset, it becomes obvious that there have been and still remain many problems that the users face. The analysis of third-party cookies clearly identifies how they are currently deployed and used, or abused, by various actors in the digital world. It is also obvious by many articles referenced that the end users are ambivalent or totally unaware of how cookies, in general, work and what they can do to prevent the exposure of their personal information to nefarious users of the internet.

The current Laws and Regulations show that they are helping to improve end user personal data security, especially when compared to before there was any oversight. However, it also shows that there are still many gaps in those laws and regulations, some that could easily be filled utilizing the currently available technology, even without new laws and regulations.

It can also be seen that there are many existing tools that can be used to help casual internet users become vastly more secure with their personal information. Again, these existing tools, such as OpenWPM, SeaMonkey, NoTrace, Acumen, Bonfire and NoScript, need to be advertised as some relatively simple security actions that they might want to take, but again a lack of education of the problems they face and solutions available to them is inhibiting the end users of browsers and web sites. The future with mobile devices and using the Cloud hold new and increasing challenges for users and therefore the regulators.

CONCLUSION

As shown in the analysis of the current situation, the research does not seem to indicate what the end users seem to prefer when it comes to the regulations provided. There seems to be no information online that compares European users to north American users when it comes to their cookie settings between sites in the different regions. This could be a good indication on what the end users seem to understand and prefer when it comes to cookie policies and which regulation seems to be preferred by the end users concerns with cookies protecting their browsing data. I feel that with the information available in the research data sets, such as the location of the user and the website could easily indicate what differences exist between the different regional users and their interactions with other regions regulations. It is understood that the users understanding of the different cookie policies will obscure the

comparison to some extent i.e., the US user may not know they have more control of cookies in the European site. In the case of a European user, they may decide not to use the site based on the lack of cookie settings. Educating the general public on this subject, and what countermeasures they can easily take, is a very simple way that governmental officials can help the consumer, which does not require changes in the law or new technology. The governments just need to inform their citizens so they can protect themselves in the digital world as soon as possible.

It can also be seen that all of the potential cookie security tools available should ultimately be made mandatory with all browsers, just like anti-lock brakes and car horns are mandatory in cars, these both help to avoid car accidents, just as making some cookie policies mandatory could help prevent personal information data breaches. These tools also need to have UI's that make them to be easy to configure and use by the "rookie" browsers user. Simply put if the browser companies were to be made more responsible for the user's personal information security over the ease and convenience of the user experience then the security situation could be vastly improved.

The study shows the understanding of the cookies' impact and finding strategies for secure, improved user experience. This study showed the acknowledgment for the dual nature of cookies, highlighting both their benefit to user experience and the potential risks they pose.

FUTURE RESEARCH

Potential future research on this could be using OpenWPM with a sample size of different website browsers and seeing the information I can collect from cookie sniffing. I could evaluate this over a long period and by reaching out to the companies to see if they can make changes so that it won't happen again

Whilst researching this paper it became apparent that there are vast amounts of research (Holz T et al, 2019) on the USA and EU cookies and even the difference in the relative laws and regulations (Perumal, V., 2022.) but there is little to no research comparing actual end user cookie interaction between US and EU users that result from the different regulations and the ways that they are implemented. As a simple start it is noted that cultural differences exist between EU and USA lawmakers in as such that the US is more hands off and favors the companies collecting the data. Simply put the US believes "The use of personal data for commercial purposes exceeds the importance of data privacy" (Krupp, N., 2009.). Although the many data breaches in the USA is bringing this philosophy into question. Several States are implementing regulations similar to the EU GDPR (Koenig, T.H., 2019), but still most states are not. This means most US users not familiar with the finer controls that the EU, and some forward-thinking US states, sites make their users accustomed to with regards to cookie control.

The bigger gap in the research is comparing how the end users in the 2 different regions are protecting themselves with the capabilities each set of regulations requires users be provided with. For instance, in the EU a user gets the cookie popup message but can then go to the *manage cookie setting page* as shown in Figure 6 below.

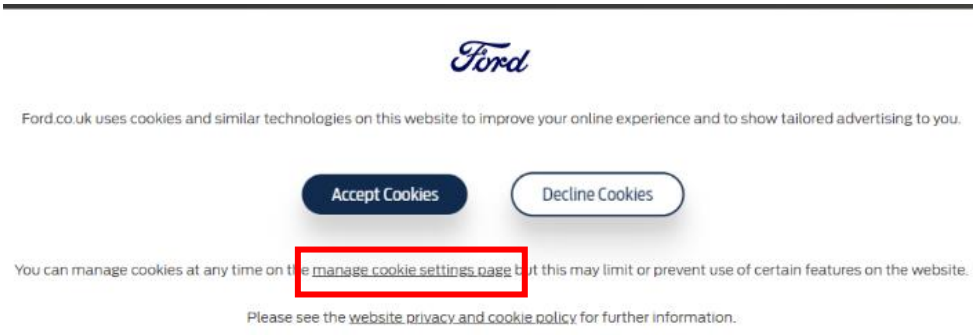


FIGURE 6: THE FORD WEBSITE IN THE EU WITH A LINK TO ANOTHER PAGE FOR THE USER TO MANAGE THEIR COOKIE PREFERENCES.

Once the manage cookie setting page is selected a user can select how to manage 4 different types of cookies the dialog describes each one and how the site owner intends to use the information, as shown in figure 7 below.

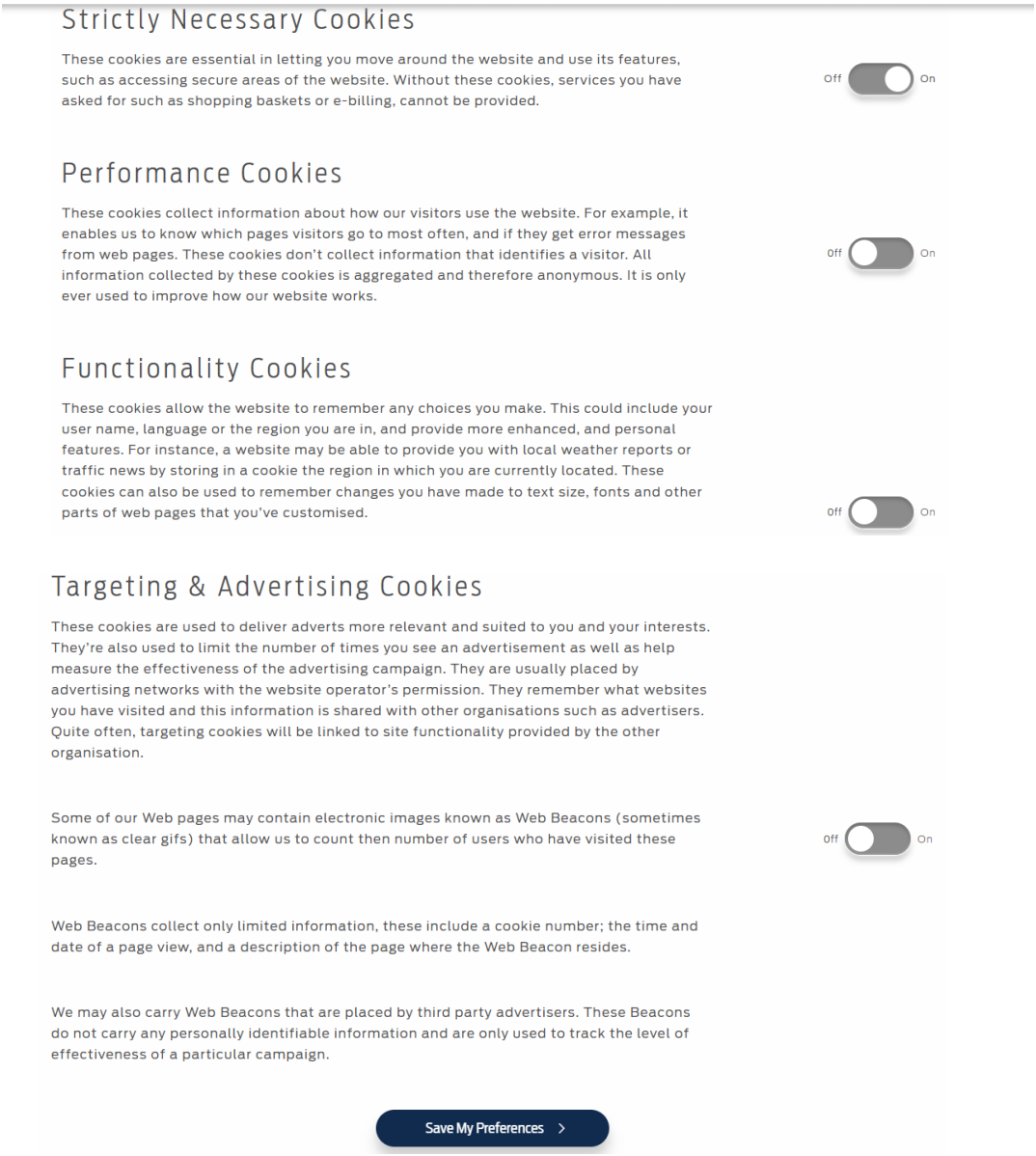


FIGURE 7: THE EU SITES COOKIE PREFERENCE SETTINGS PAGE SHOWS 4 SEPARATE TYPES OF COOKIES AND FULLY EXPLAINS THEIR USE AND CONSEQUENCES OF INCLUSION.

Research has shown that most EU site users do not accept the tracking type of cookies (Schaub et al. 2019). But in the USA a user does not even get that option they basically can opt in or out of using cookies, this is show in figure 8 below.

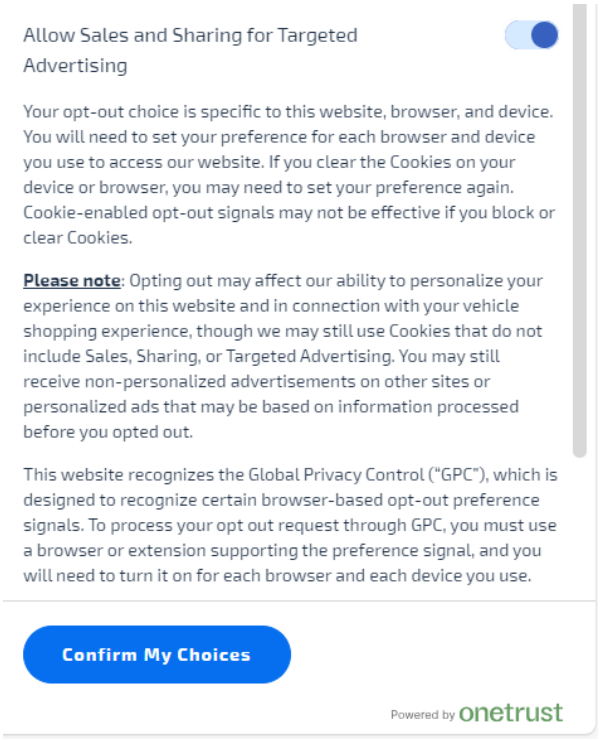


FIGURE 8: EXAMPLE OF THE SAME COMPANIES US SITES COOKIE PAGE WITH THE LIMITED SELECTIONS AVAILABLE TO THE USER.

Therefore, EU users seem to be better informed on each type and can control how they interact with each type, but the US users are not educated by their cookie dialog and are left with an all or nothing selection.

This research should look deeper and compare users that reside in the 2 different domains by noting where the EU site user resides because we could then see if users that reside in the US are using the extra enhanced cookie features provided on the EU site. Even this will not be comprehensive as the US

residents are not used to being offered the extra capability and could quite often just accept / reject all and not go to the *manage cookie setting page*.

The bigger gap in the research is how users from the EU and US treat the different regulations. This would give some simple insight on how effective each set of regulations & their implementations are working for the end users. Specifically, how do EU users oversee the reduced cookie control on US sites and how do US users manage the increased cookie control when visiting EU sites. This could indicate if EU users are better informed on cookies that US users because they either reject or accept the cookie settings in the EU sites. The research can also indicate if US users seems to utilize the extra cookie control when offered at EU sites thus indicating a desire for better cookie policies and implementation in the US than they currently have

The EU users do not like to be tracked because they are told about the different cookie types and can be selective there is no research there is no possibility to see what the US users would do with that level of control, but it does seem that the users that have that level of control do use it in the EU. Therefore, it seems as though the US regulators are not providing the US site users with enough protection.

REFERENCES

Kulyk, O., Hilt, A., Gerber, N. and Volkamer, M., 2018, April. this website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In the European Workshop on Usable Security (EuroUSEC) (Vol. 4).

Cahn, A., Alfeld, S., Barford, P. and Muthukrishnan, S., 2016, April. An empirical study of web cookies. In *Proceedings of the 25th international conference on world wide web* (pp. 891-901).

Dao, H. and Fukuda, K., 2021, December. Alternative to third-party cookies: investigating persistent PII leakage-based web tracking. In *Proceedings of the 17th International Conference on emerging Networking EXperiments and Technologies* (pp. 223-229).

Gotze, M., Matic, S., Iordanou, C., Smaragdakis, G. and Laoutaris, N., 2022, June. Measuring Web Cookies in Governmental Websites. In *14th ACM Web Science Conference 2022* (pp. 44-54).

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T., 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096*.

Etzioni, A., 2011. The privacy merchants: What is to be done. *U. Pa. J. Const. L.*, *14*, p.929.

Khu-Smith, V. and Mitchell, C., 2002. Enhancing the security of cookies. In *Information Security and Cryptology—ICISC 2001: 4th International Conference Seoul, Korea, December 6–7, 2001 Proceedings 4* (pp. 132-145). Springer Berlin Heidelberg

Pantelic, O., Jovic, K. and Krstovic, S., 2022. Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations. *Sustainability*, *14*(9), p.5015.

Sudhodanan, A. and Paverd, A., 2022. Pre-hijacked accounts: An Empirical Study of Security Failures in User Account Creation on the Web. In *31st USENIX Security Symposium (USENIX Security 22)* (pp. 1795-1812).

Zimmeck, S., Li, J.S., Kim, H., Bellovin, S.M. and Jebara, T., 2017, August. A Privacy Analysis of Cross-device Tracking. In *USENIX Security Symposium* (Vol. 17).

Trevisan, M., Stefano, T., Bassi, E. and Marco, M., 2019. 4 years of EU cookie law: Results and lessons learned. *Proceedings on Privacy Enhancing Technologies*, *2019*(2), pp.126-145.

Malandrino, D., Petta, A., Scarano, V., Serra, L., Spinelli, R. and Krishnamurthy, B., 2013, November. Privacy awareness about information leakage: Who knows what about me? In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society* (pp. 279-284).

Kumawat, N., Chaudhary, R., and Tiwari, A.K.,2 022 March A Case Study on Cookies and Cyber Security.

Goecks, J., Edwards, W.K. and Mynatt, E.D., 2009, July. Challenges in supporting end-user privacy and security management with social navigation. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (pp. 1-12).

Roesner, F., Kohno, T. and Wetherall, D., 2012. Detecting and defending against third-party tracking on the web. In *Presented as part of the 9th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 12)* (pp. 155-168).

Yu, Z., Macbeth, S., Modi, K. and Pujol, J.M., 2016, April. Tracking the trackers. In *Proceedings of the 25th International Conference on World Wide Web* (pp. 121-132).

Eckersley, P., 2010. How unique is your web browser? In *Privacy Enhancing Technologies: 10th International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings 10* (pp. 1-18). Springer Berlin Heidelberg.

Merzdovnik, G., Huber, M., Buhov, D., Nikiforakis, N., Neuner, S., Schmiedecker, M. and Weippl, E., 2017, April. Block me if you can: A large-scale study of tracker-blocking tools. In *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 319-333). IEEE.

Libert, T., 2015. Exposing the hidden web: An analysis of third-party HTTP requests on 1 million websites. *arXiv preprint arXiv:1511.00619*.

Urban, T., Degeling, M., Holz, T. and Pohlmann, N., 2020, April. Beyond the front page: Measuring third-party dynamics in the field. In *Proceedings of The Web Conference 2020* (pp. 1275-1286).

Sivakorn, S., Polakis, I. and Keromytis, A.D., 2016, May. The cracked cookie jar: HTTP cookie hijacking and the exposure of private information. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 724-742). IEEE.

Elmér, J. and Nilsson, J., 2023. *A FUTURE WITHOUT THIRD-PARTY COOKIES A study of how Swedish small and medium-sized marketing agencies are affected by the loss of third-party cookies and how potential change strategies are communicated* (Master's thesis).

Krishnamurthy, B., Malandrino, D. and Wills, C.E., 2007, July. Measuring privacy loss and the impact of privacy protection in web browsing. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 52-63).

Jackson, C., Bortz, A., Boneh, D. and Mitchell, J.C., 2006, May. Protecting browser state from web privacy attacks. In *Proceedings of the 15th international conference on World Wide Web* (pp. 737-744).

Acar, G., Eubank, C., Englehardt, S., Juarez, M., Narayanan, A. and Diaz, C., 2014, November. The web never forgets: Persistent tracking mechanisms in the wild. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 674-689).

Zhu, J. and Desai, B.C., 2015, July. User agent and privacy compromise. In *Proceedings of the Eighth International C* Conference on Computer Science & Software Engineering* (pp. 38-45).

Shah, M.A., Swaminathan, R. and Baker, M., 2008. Privacy-preserving audit and extraction of digital contents. *Cryptology ePrint Archive*.

Oksanen, T., 2022. Companies' maturity for the deprecation of third-party cookies.

Gardner, G.J., 2021. Aiding and abetting: Third-party tracking and (in) secure connections in public libraries. *The Serials Librarian*, *81*(1), pp.69-87.you

Mellet, K. and Beauvisage, T., 2020. Cookie monsters. Anatomy of a digital market infrastructure. *Consumption Markets & Culture*, *23*(2), pp.110-129.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. and Molina, J., 2009, November. Controlling data in the cloud: outsourcing computation without outsourcing control. In *Proceedings of the 2009 ACM workshop on Cloud computing security* (pp. 85-90).

Kristol, D.M., 2001. HTTP Cookies: Standards, privacy, and politics. *ACM Transactions on Internet Technology (TOIT)*, *1*(2), pp.151-198.

Agarwal, L., Shrivastava, N., Jaiswal, S. and Panjwani, S., 2013, July. Do not embarrass: Re-examining user concerns for online tracking and advertising. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (pp. 1-13).

Han, S., Jung, J. and Wetherall, D., 2012. A study of third-party tracking by mobile apps in the wild. *Univ. Washington, Tech. Rep. UW-CSE-12-03*, *1*.

Mayer, J.R. and Mitchell, J.C., 2012, May. Third-party web tracking: Policy and technology. In *2012 IEEE symposium on security and privacy* (pp. 413-427). IEEE.

Englehardt, S. and Narayanan, A., 2016, October. Online tracking: A 1-million-site measurement and analysis. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 1388-1401).

Belloro, S. and Mylonas, A., 2018. I know what you did last summer: New persistent tracking mechanisms in the wild. *IEEE Access*, *6*, pp.52779-52792.

Geradin, D., Katsifis, D. and Karanikioti, T., 2020. Google as a de facto privacy regulator: Analyzing Chrome's removal of third-party cookies from an antitrust perspective.

Hormozi, A.M., 2005. Cookies and privacy. *Information Security Journal*, *13*(6), p.51.

Lin, D. and Loui, M.C., 1998. Taking the byte out of cookies: privacy, consent, and the Web. *ACM SIGCAS Computers and Society*, *28*(2), pp.39-51.

Ayenson, M.D., Wambach, D.J., Soltani, A., Good, N. and Hoofnagle, C.J., 2011. Flash cookies and privacy II: Now with HTML5 and ETag respawning. *Available at SSRN 1898390*.

Pierson, J. and Heyman, R., 2011. Social media and cookies: challenges for online privacy. *info*.

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G. and Weippl, E., 2019. Measuring cookies and web privacy in a post-GDPR world. In *Passive and Active Measurement: 20th International Conference, PAM 2019, Puerto Varas, Chile, March 27–29, 2019, Proceedings 20* (pp. 258-270). Springer International Publishing.

Shankar, S., Sinha, R., Mitra, S., Swaminathan, V., Mahadevan, S. and Sinha, M., 2023, February. Privacy Aware Experiments without Cookies. In *Proceedings of the Sixteenth ACM International Conference on Web Search and Data Mining* (pp. 1144-1147).

Park, J.S. and Sandhu, R., 2000. Secure cookies on the Web. *IEEE internet computing*, *4*(4), pp.36-44.

Sit, E. and Fu, K., 2001. Inside risks: Web cookies: not just a privacy risk. *Communications of the ACM*, *44*(9), p.120.

Kulyk, O., Hilt, A., Gerber, N. and Volkamer, M., 2018, April. this website uses cookies": Users' perceptions and reactions to the cookie disclaimer. In *European Workshop on Usable Security (EuroUSEC)* (Vol. 4).

Schmidt, L., Bornschein, R. and Maier, E., 2020. The effect of privacy choice in cookie notices on consumers' perceived fairness of frequent price changes. *Psychology & Marketing*, *37*(9), pp.1263-1276.

Aladeokin, A., Zavarsky, P. and Memon, N., 2017, September. Analysis and compliance evaluation of cookies-setting websites with privacy protection laws. In *2017 Twelfth International Conference on Digital Information Management (ICDIM)* (pp. 121-126). IEEE.

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), pp.135-154.

Pantelic, O., Jovic, K. and Krstovic, S., 2022. Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations. *Sustainability*, *14*(9), p.5015.

Dabrowski, A., Merzdovnik, G., Ullrich, J., Sendera, G. and Weippl, E., 2019. Measuring cookies and web privacy in a post-GDPR world. In *Passive and Active Measurement: 20th International Conference, PAM 2019, Puerto Varas, Chile, March 27–29, 2019, Proceedings 20* (pp. 258-270). Springer International Publishing.

Pierson, J. and Heyman, R., 2011. Social media and cookies: challenges for online privacy. *info*.

Luzak, J.A., 2014. Privacy notice for dummies? Towards European guidelines on how to give "clear and comprehensive information" on the cookies' use in order to protect the internet users' right to online privacy. *Journal of Consumer Policy*, *37*, pp.547-559.

Debusseré, F., 2005. The EU e-privacy directive: a monstrous attempt to starve the cookie monster? *International journal of law and information technology*, *13*(1), pp.70-97.

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), pp.135-154.

Kretschmer, M., Pennekamp, J. and Wehrle, K., 2021. Cookie banners and privacy policies: Measuring the impact of the GDPR on the web. *ACM Transactions on the Web (TWEB)*, *15*(4), pp.1-42.

Jayakumar, L.N., 2021. Cookies 'n'Consent: An empirical study on the factors influencing of website users' attitude towards cookie consent in the EU. *DBS Business Review*, *4*.

Schmidt, L., Bornschein, R. and Maier, E., 2020. The effect of privacy choice in cookie notices on consumers' perceived fairness of frequent price changes. *Psychology & Marketing*, *37*(9), pp.1263-1276.

Etzioni, A., 2011. The privacy merchants: What is to be done. *U. Pa. J. Const. L.*, *14*, p.929.

Hu, X., Sastry, N. and Mondal, M., 2021, June. Cccc: Corralling cookies into categories with cookiemonster. In *13th ACM Web Science Conference 2021* (pp. 234-242).

Pantelic, O., Jovic, K. and Krstovic, S., 2022. Cookies implementation analysis and the impact on user privacy regarding GDPR and CCPA regulations. *Sustainability*, *14*(9), p.5015.

Van Eijk, R., Asghari, H., Winter, P. and Narayanan, A., 2021. The impact of user location on cookie notices (inside and outside of the European Union). *arXiv preprint arXiv:2110.09832*.

Hu, X. and Sastry, N., 2019, June. Characterising third-party cookie usage in the EU after GDPR. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 137-141).

Cozza, F., Guarino, A., Isernia, F., Malandrino, D., Rapuano, A., Schiavone, R. and Zaccagnino, R., 2020. Hybrid and lightweight detection of third-party tracking: Design, implementation, and evaluation. *Computer Networks*, *167*, p.106993.

Mayer-Schonberger, V., The Internet, and Privacy Legislation: Cookies for a Treat&quest.

Yue, C., Xie, M. and Wang, H., 2010. An automatic HTTP cookie management system. *Computer Networks*, *54*(13), pp.2182-2198.

Leenes, R. and Kosta, E., 2015. Taming the cookie monster with dutch law–a tale of regulatory failure. *Computer Law & Security Review*, *31*(3), pp.317-335.

Kierkegaard, S.M., 2005. How the cookies (almost) crumbled: Privacy & lobbyism. *Computer Law & Security Review*, *21*(4), pp.310-322.

Binns, R. and Bietti, E., 2020. Dissolving privacy, one merger at a time: Competition, data, and third-party tracking. *Computer Law & Security Review*, *36*, p.105369.

Vitunskaite, M., He, Y., Brandstetter, T. and Janicke, H., 2019. Smart cities and cyber security: Are we there yet? A comparative study on the role of standards, third-party risk management and security ownership. *Computers & Security*, *83*, pp.313-331.

Binns, R., Lyngs, U., Van Kleek, M., Zhao, J., Libert, T. and Shadbolt, N., 2018, May. third-party tracking in the mobile ecosystem. In *Proceedings of the 10th ACM Conference on Web Science* (pp. 23-31).

Utz, C., Degeling, M., Fahl, S., Schaub, F. and Holz, T., 2019, November. (Un) informed consent: Studying GDPR consent notices in the field. In *Proceedings of the 2019 acm sigsac conference on computer and communications security* (pp. 973-990).

Perumal, V., 2022. The Future of US Data Privacy: Lessons from the GDPR and State Legislation. *Notre Dame J. Int'l Comp. L.*, *12*, p.99.

Movius, L.B. and Krup, N., 2009. US and EU privacy policy: Comparison of regulatory approaches. *International Journal of Communication*, *3*, p.19.

Rustad, M.L. and Koenig, T.H., 2019. Towards a global data privacy standard. *Fla. L. Rev.*, *71*, p.365.

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F. and Holz, T., 2018. We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy. *arXiv preprint arXiv:1808.05096*.

Zheng, X., Jiang, J., Liang, J., Duan, H., Chen, S., Wan, T. and Weaver, N., 2015. Cookies Lack Integrity:{Real-World} Implications. In *24th USENIX Security Symposium (USENIX Security 15)* (pp. 707-721).